USSTRATCOM

Global Innovation and Strategy Center

Measuring the Health of the

Global Information Grid

Spring 2009 – Project 09-01

May 2009

Intern Researchers:

Jason Cantone
Natasha Fields
Brandon Iske
Kristin Phaneuf
Karen Poyer
Daniel Reynoso
Ann Sawatzki

Project Management and Oversight:

John G. Hudson II, Ph.D.
Sarah Mussoni, M.Ed.
Kristen Rodgers

Approved: Tom Gilbert, Col, USAF
Director, Global Innovation and Strategy Center

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2009	FINAL REPORT	JANUARY 2009 - MAY 2009

4. TITLE AND SUBTITLE

Measuring the Health of the Global Information Grid

5a. CONTRACT NUMBER

N/A

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

Jason Cantone, Natasha Fields, Brandon Iske, Kristin Phaneuf, Karen Poyer, Daniel Reynosa, Ann Sawatzki

5d. PROJECT NUMBER

09-01

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
Intern Program
6805 Pine Street
Omaha, NE 68106

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
Intern Program
6805 Pine Street
Omaha, NE 68106

10. SPONSOR/MONITOR'S ACRONYM(S)

USSTRATCOM - GISC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Monitoring the health of the GIG is one of the most critical aspects of operationalizing cyber missions. This report focuses on the health of the Global Information Grid (GIG), a globally interconnected Department of Defense (DoD) network (of systems) that collects, processes, and manages information for warfighters, policymakers, and support personnel. The three primary components of GIG health (as defined by the customer) include sustainability, reliability and survivability. Sustainability is the consistent performance of network tasks over time; whereas reliability is the accuracy, accessibility and obtainability of information for the user; and survivability being the availability of alternate data route despite internal/external issues. The focus of the project was to design a framework for metrics to assess the health of the GIG. Private sector metrics were extrapolated to measure the sustainability, reliability, and survivability of the GIG and were included as commercial best practices. Also investigated were internal and external threats, such as interference, intrusion, and malicious activity (e.g., cyber-terrorists) that could undermine the system's capability.

15. SUBJECT TERMS

Global Information Grid, GIG, health index, metrics, network, cyber, Network-Centric Warfare, Internet, interference, intrusion, malicious, grid health, sustainability, reliability, survivability, Information Assurance, IA, query, attribution, culture, hacker, threat, framework, user accountability, attack

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. John G. Hudson II
U	U	U	UU	105	19b. TELEPHONE NUMBER *(Include area code)* 402-398-8034

For additional information or questions concerning this report, please contact the following individuals:

Intern Program Manager:
John G. Hudson II, Ph.D., YA-02, DAF
Commercial (402) 398-8034
John.Hudson@thegisc.org
John.Hudson@stratcom.mil

Intern Program Administration:
Sarah Mussoni, M.Ed, YA-02, DAF
Commercial (402) 398-8028
Sarah.Mussoni@thegisc.org
Sarah.Mussoni@stratcom.mil

GISC Innovation Division Chief:
Ms. Elizabeth Durham-Ruiz, YF-03, DAF
Commercial (402) 398-8022
elizabeth.durhamruiz@thegisc.org
Durhame@stratcom.mil

GISC Innovation Deputy Division Chief:
Mr. Ron Moranville, YA-02, DAF
Commercial (402) 398-8021
ron.moranville@thegisc.org
Moranvil@stratcom.mil

TABLE OF CONTENTS

FIGURES

ACRONYMS

AFIT	Air Force Institute of Technology
AFRL	Air Force Research Laboratory
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
BACN	Battlefield Airborne Communications Node
CCA	Clinger-Cohen Act
CIA	Central Intelligence Agency
CPU	Central Processing Unit
CRD	Capstone Requirements Document
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DoI	Department of the Interior
DoJ	Department of Justice
DoL	Department of Labor
DoS	Department of State
DoT	Department of Transportation
ED	Department of Education
EPRI	Electrical Power Research Institute Equipment Superior to Operator
ESSG	Enterprise-Wide IA and CND Solutions Steering Group
FCIV	File Checksum Integrity Verifier Global Information Grid
GIG	Global Information Grid
HBSS	Host-Based Security System
HHS	Department of Health and Human Services
HTTPS	HyperText Transfer Protocol Secure
HUD	Department of Housing and Urban Development
IA	Information Assurance
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunications Union
JTF-GNO	Joint Task Force, Global Network Operations
JTRS	Joint Tactical Radio System
MD5	Message-Digest algorithm 5 (MD5)

MLPP	Multi-Level Precedence and Preemption
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
NCO	Net-Centric Operations
NCOW	Network-Centric Operations and Warfare
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
PC	Personal Computer
QoS	Quality of Service
RFC	Request for Comments
SCADA	Supervisory Control and Data Acquisitions
SHA-1	Secure Hash Algorithm 1
SIPRNET	Secret Internet Protocol Router Network
SM	Simulated Machines
SOA	Service-Oriented Architecture
SONET	Synchronous Optical Networks
SRMM/p	Parametric State Reward Markov Model
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol /Internet Protocol
TSAT	Transformational Satellite
UAV	Unmanned Aerial Vehicle
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USDA	US Department of Agriculture
USSTRATCOM	U.S. Strategic Command
VA	Department of Veteran's Affairs
VMP	Virtual Message Processor
VoIP	Voice over Internet Protocol
VPN	Virtual Private Networks
WEP	Wired Equivalent Privacy
WHO	World Health Organization

PREFACE

This report is the product of the United States Strategic Command (USSTRATCOM) Global Innovation and Strategy Center (GISC) internship program. A team of graduate and undergraduate students from the University of Nebraska-Lincoln, University of Nebraska-Omaha, and Creighton University worked together with the goal of providing a multidisciplinary, unclassified, non-military perspective on important Department of Defense issues pertaining to protecting the Global Information Grid (GIG).

The Spring 2009 team was charged with analyzing the specific difficulties associated with measuring the health of the Global Information Grid (GIG) and networks in relation to the already accepted terms of Sustainability, Reliability, and Survivability. These terms were presented to the research team from the customer of the project. The focus of the project was to design a framework for metrics to assess the health of the GIG considering sustainability, reliability, and survivability.

This project occurred between January and early May 2009, with each team member working twelve to twenty hours per week. While the GISC provided the resources and technology for the project, it was solely up to the team to develop the project design, conduct the research and analysis, and provide appropriate recommendations.

EXECUTIVE SUMMARY

The Global Information Grid (GIG) is a globally interconnected Department of Defense (DoD) network (of systems) that collects, processes, and manages information for warfighters, policymakers, and support personnel. The GIG provides a critical foundation for the DoD Net-Centric Operations (NCO) by connecting people and systems regardless of time or place, and providing vastly superior situational awareness and better access to information for more effective decision-making. The ability for the GIG to operate seamlessly is impacted by interference, intrusions, and other malicious activities. Monitoring the health of the GIG is one of the most critical aspects of operationalizing the cyber missions.

A framework of metrics must be addressed to measure GIG health. The basic tenants of measuring the health of the GIG, as defined by the customer are: sustainability, reliability and survivability: which make them the basis for the team's metrics.

The focus of the project was to design a framework for metrics to assess the health of the GIG considering sustainability, reliability, and survivability.

The team first defined sustainability, reliability, and survivability to create a common lexicon to guide future discussions of how these components impact GIG health

- Sustainability: consistent performance of network tasks over time
- Reliability: accuracy, accessibility and obtainability of information for the user
- Survivability: availability of alternate data route despite internal/external issues

The team then researched metrics in which to measure the health of the GIG. Private sector metrics were extrapolated to measure the sustainability, reliability, and survivability of the GIG and were included as commercial best practices. Also investigated were internal and external threats that could undermine the system's capability.

The team was allotted 120 days to conduct open-source research using all available information sources, write a comprehensive report, and provide an executive briefing to the U.S. Strategic Commander and Staff, U.S. Government agencies, and other interested parties.

The team proposed six strategies to support the overall health of the GIG:

- Acknowledge unitary control of the GIG
- Enforce user accountability
- Use common definitions, language, and measurement
- Encourage collaboration among organizations contributing information
- Weigh mission necessity more heavily than user rank
- Implement team's "notional" health indicator

INTRODUCTION

The Global Information Grid (GIG) is an extraordinarily complex Department of Defense (DoD) "undertaking" with the objective of integrating all types of systems and data into a single, reliable network.[1] The ideal GIG is a system of systems, an enormous network that contains a wide range of technology and a variety of users. As defined by DoD Directive 8100.1, it is:

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority.[2]

The ideal GIG is modeled after the current Internet system, where the ultimate goal is to have limitless information instantaneously available from any location, provided one has the proper security clearance and priority.[3] Charles P. Satterthwaite, an electrical engineer at the Air Force Research Laboratory (AFRL), provides an easy to understand explanation of informational systems. He states that the Infosphere, like the GIG, can be considered the "Internet In The

[1] Chaplain, Cristina, et al. "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation." U.S. Government Accountability Office. 13 May 2009 <http://www.gao.gov/new.items/d04858.pdf>.
[2] Wolfowitz, Paul. "Global Information Grid (GIG) Overarching Policy." Department of Defense Directive 8100.1. 13 May 2009 <http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf>.
[3] Satterthwaite,Charles P. "Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid." Defense Technical Information Center. 13 May 2009 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468199&Location=U2&doc=GetTRDoc.pdf>.

Sky."[4] The Internet provides worldwide access to telecommunication systems which contain essential information regarding such issues as national security. However, the Infosphere is more multi-dimensional than the Internet. Not only would GIG users be connected to the Internet, they would also be "plugged into multiple information sources . . . which are time tagged, integrated, and filtered to give expanded real-time (or near real-time) solutions."[5] Ideally, this becomes a "publish and subscribe" or "plug and play" network where any necessary application can be implemented locally and accessed worldwide "to help achieve war-fighting objectives."[6] According to the GIG Architectural Vision:

> GIG capabilities are effectively aligned to enable a dynamic and responsive end-to-end operational environment, (1) where information is available (2) the means to produce, exchange, and use information are assured and protected; and (3) where resources such as bandwidth, spectrum, and computing power are dynamically located based on mission requirements.[7]

This new information-based concept requires a shift away from a need-to-know policy and cultural model, and a shift towards a need-to-share model requiring significant change in the current defense and intelligence culture.[8] Increased information-sharing capabilities would allow users to access needed information quickly and in a reliable manner, resulting in quicker, more informed, and timely decision making. The increased availability of information would also allow for warfighters to correctly "[identify] threats more effectively, making informed

---

[4] Satterthwaite,Charles P. "Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid." Defense Technical Information Center. 13 May 2009 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468199&Location=U2&doc=GetTRDoc.pdf>.
[5] Satterthwaite, Charles P.
[6] White, B. E. "Layered Communications Architecture for the Global Grid." MITRE Corporation. 13 May 2009 < http://www.mitre.org/work/tech_papers/tech_papers_01/white_layered/white_layered.pdf>.
[7] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.
[8] DoD CIO.

decisions, and responding with greater precision and lethality."[9] However, it is important to distinguish between the ideal GIG and the GIG as it is today. The ideal GIG, shown in Figure 1, consists of a connected system comprised of space, airborne, wireless, and radio segments which has not yet been fully realized, while the current GIG is a fractured system of several disconnected domains.[10]

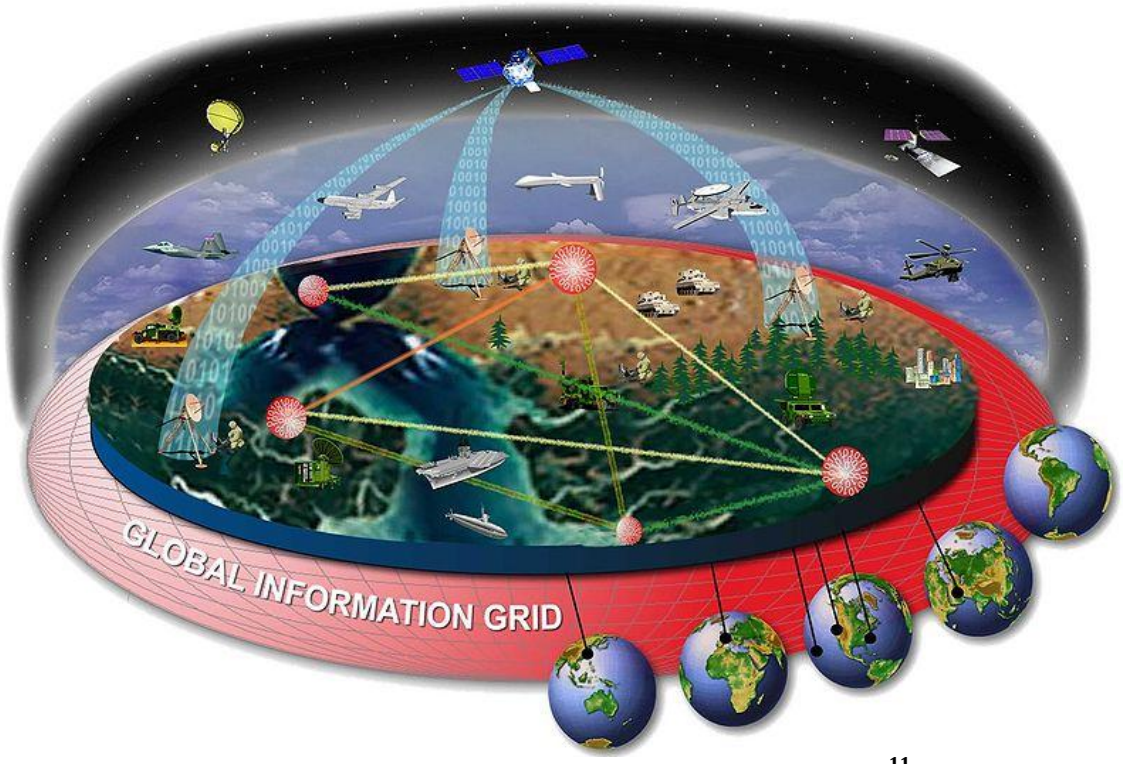

Figure 1: Illustration Representing the Ideal GIG[11]

[9] Chaplain, Cristina, et al. "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation." U.S. Government Accountability Office. 13 May 2009 <http://www.gao.gov/new.items/d04858.pdf>.
[10] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.
[11] "Global Information Grid Digital image." Wright-Patterson Air Force Base. 17 May 2009 <http://www.wpafb.af.mil/shared/media/photodb/photos/060629-F-7777J-025.jpg>.

Network-Centric Warfare: The Driving Force behind the GIG

Network-Centric Operations and Warfare (NCOW) is the doctrine driving the shift from traditional warfare to information-based cyber-warfare. According to Mr. John Luddy, an Adjunct Fellow at the Lexington Institute:

> The goal of network-centric operations is to enable forces to accomplish their objectives more efficiently: faster; with fewer troops in harm's way; and with fewer and lighter weapons and other equipment to bring to, sustain, and maneuver in the battlespace. With timely and accurate intelligence, commanders can decide faster, deploy a force of the optimal size and characteristics, command and control that force better, and stay one step ahead of enemy forces.[12]

The ability to access the needed information in a timely manner enables warfighters to make quick, informed decisions, reducing overall costs and resulting in greater preemptive capabilities and lethality. For example, if a covert operation was happening overseas, the warfighter would ideally be able to access information about the enemy's location, supply chain, and weapons and technological capabilities almost instantaneously. From there the warfighter could make informed decisions about where a strike would be most detrimental to the enemy force. In Luddy's publication, the benefits of NCOW to a major theatre operation are apparent when analyzing the shift from the more traditional mode of warfare in Operation Desert Storm (1991) to the information-based warfare capabilities used in Operation Iraqi Freedom (2003).[13] It can be concluded that the GIG is the physical embodiment of NCOW, creating system and worldwide

[12] Luddy, John. "The Challenge and Promise of Network-Centric Warfare." Lexington Institute. 16 May 2009 <http://www.lexingtoninstitute.org/docs/521.pdf>.
[13] Luddy, John.

interoperability, a communications and intelligence system, and most significantly, a weapons system.

Purpose of the GIG

Dialogue regarding capabilities appeared to be endless during initial discussions and planning sessions for the GIG. For example, Charles Satterthwaite stated that "the expectation of the Global Grid is that it will be able to provide accurate, secure, and timely information to our commanders anywhere, anytime, and in their specific information application requirement."[14] This expectation requires a deeper understanding of not only innovative technologies, but also a comprehensive understanding of each information platform so that effective integration can occur. The GIG does not solely cover one network or operational system. Instead, it provides a layered framework to facilitate communication between multiple functions and protocols. This layering is a technical architecture, not an operational or systems architecture, aimed at achieving *horizontal* integration of military communications.[15] The technical architecture of the GIG differs from the historically *vertical* approach of the DoD communication system. B.E. White stated that principal benefit of this layering approach is the ability to upgrade technology within a given layer without disrupting the entire system.[16]

In particular, the GIG has application to the Aerospace Command and Control and Intelligence, Surveillance, and Reconnaissance (C2ISR) Campaign Plan of 2000. Satterthwaite explains that while almost a decade old, this plan showcases that the GIG contains highly sensitive material of

---

[14] Satterthwaite,Charles P. "Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid." Defense Technical Information Center. 13 May 2009 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468199&Location= U2&doc=GetTRDoc.pdf>.
[15] White, B. E. "Layered Communications Architecture for the Global Grid." MITRE Corporation. 13 May 2009 < http://www.mitre.org/work/tech_papers/tech_papers_01/white_layered/white_layered.pdf>.
[16] White, B. E.

national importance that must be maintained within a healthy, secure network environment free from cyber threats and reliable in times of need. Looking in depth to the C2ISR plan, the goal of the GIG is to "obtain seamless, protected, reliable, worldwide connectivity to support… mission needs."[17]

Components of the GIG

The GIG consists of the three major components hardware, data, and users. Hardware is the system itself and it incorporates a range of technology too great to detail completely in this report. According to the Air Force Institute of Technology (AFIT), this technology is categorized into the following four layers: surface, aerospace, near-space, and satellite.[18] The surface layer includes both fixed communications (i.e., base or fixed node) and mobile communications from actively moving troops, aircraft, or maritime craft. An example is the Joint Tactical Radio System (JTRS), which is the main communication system between the varying GIG layers and levels of technology. It allows a bridging of "interoperability gaps between current users and new Internet Protocol (IP) terminals for mobile users on the ground, at sea, or in the air, as well as connect those same users to a permanent terrestrial network."[19] The aerospace layer consists mainly of aircraft (e.g., helicopters, cargo planes, fighters) and is traditionally used for intelligence, surveillance, and reconnaissance. With the advent of the Battlefield Airborne Communications Node (BACN), technology should take on further roles that will provide

[17] Satterthwaite,Charles P. "Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid." Defense Technical Information Center. 13 May 2009 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468199&Location=U2&doc=GetTRDoc.pdf>.
[18] Hubenko, Victor P., et al. "Improving the Global Information Grid's Performance through Satellite Communications Layer Enhancements." IEEE Communications Magazine Nov. 2006.
[19] Hubenko, Victor P., et al.

communication connections between the aerospace and surface layers.[20] Major Hubenko, an AFIT graduate, disclosed that the near-space layer has been widely underutilized thus far but is expected to be further developed as there are many advantages in doing so. These advantages include decreased financial cost of development and operation due to the actual placement and proximity of the technology closer to earth (as opposed to further out in space), increased performance of such devices due to less distortion and interference, and less damage to equipment from weather. The near-space layer of technology includes devices similar to unmanned aerial vehicles (UAV), aircraft, and other vehicles that can be piloted from a remote location—some of which have yet to be developed fully.[21] The satellite layer is essential to the seamless functioning of the GIG and encompasses a wide range of developed and developing technologies, thus providing "the military with narrowband, wide-band, and protected communications capabilities."[22] Although there are many technologies in place, it is uncertain where many other programs stand in their development. For example, the Transformational Satellite (TSAT) program that is intended to extend the data transmission capabilities and speed within the GIG, nearing real-time speeds and allowing for quick, informed decision-making, has been put on hold several times since its inception in 2004. The initial 2011 launch of the TSAT has been pushed back to 2014 due to budget cuts and insufficient information about TSAT technology.[23] Due to the various layers within the GIG and the enormous array of technology, measuring the health of the GIG becomes quite a challenge. This challenge becomes even more difficult when such aspects as the size and type of data and the user are considered.

---

[20] Hubenko, Victor P., et al. "Improving the Global Information Grid's Performance through Satellite Communications Layer Enhancements." IEEE Communications Magazine Nov. 2006.
[21] Hubenko, Victor P., et al.
[22] Hubenko, Victor P., et al.
[23] Gallegos, Arthur, et al. "Space Acquisitions: GAO-06-537 Space Acquisitions: DoD needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications Systems." U.S. Government Accountability Office. 16 May 2009 <http://www.gao.gov/new.items/d06537.pdf>.

Before discussing the framework for metrics to measure the health of the GIG, data and users should be examined. The GIG Architectural Vision identifies the ability to "fully leverage the power of information and collaboration . . ." as the target vision for the GIG.[24] Therefore it can be said that data is the most important component of the GIG, and requires the most protection and attention. Data is what makes the GIG a system for communication as well as a weapons system. It is important to remain cognizant that not all data requires the same amount of, and methods for, protection. Consideration should also be devoted to who (i.e., individual user or organization) is contributing or sharing data, and the implications of that contribution or sharing of data to the overall system. According to Gary Buda of Booz Allen Hamilton, the three different types of network traffic (or data) within systems are the user, control, and management communications.[25] User traffic is information due to users or user applications; for example, a program that a user controls is transmitting over a network. Control traffic is information being transmitted that is essential to ensuring the user is connected to the network, such as the automated processes the computer must complete to ensure connection. Management traffic is information about the status and performance of the network itself, such as updates about vulnerabilities in the network's infrastructure or security information.[26] The three types of data are vital to the successful functioning of the GIG; however, it is necessary to determine what type of user data in particular should be protected as some pieces alone are harmless, and others may be threatening to national security if delivered to an adversary. It is crucial to determine how this data should be protected, whether via encryption, firewalls and anti-virus software,

[24] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.
[25] Buda, Gary, et al. "Security Standards for the Global Information Grid." IEEE. 21 Jan. 2009 <http://http://ieeexplore.ieee.org.leo.lib.unomaha.edu/stamp/stamp.jsp?tp=&arnumber=985877&isnumber=21247>.
[26] Buda, Gary, et al.

regular system health checks, or a combination strategy. These are just a few examples of how data can be protected. Additional techniques and specific metrics are provided throughout the report. When assessing data security, it is also important to take notice of the data contributor as well as that person's motivations and goals. U.S. government agencies are not the only contributors since "many networks used by Government agencies within the GIG have outsourced their network management services" resulting in approximately 95% of GIG transmissions taking place over commercial carriers.[27] Portions of the private sector, such as banking and medical, are incorporated into the GIG. The end-result is a largely heterogeneous variety of data, which implies that it cannot all be handled in a uniform way. Again, deciding what data to protect is of utmost importance

Extensive research and discussions with various experts revealed that users are among the greatest threats and vulnerabilities to the GIG. It has become more generally accepted that, "[h]uman error is now the primary cause of network downtime, whether or not the industry is prepared to admit it."[28] An example is "stupid user tricks" that include actions like bypassing security procedures with the use of thumb drives, leaving one's computer station unattended, opening emails from unknown sources, and downloading information to personal devices to finish work at home—the list of "tricks" is endless. According to Steve Broadhead, Director of the independent network testing lab Broadband-Testing, the majority of the problems at end-user organizations are a result of incorrectly configured devices—this directly translates to human error.[29] An extreme but valid example of a "stupid user trick" occurred during Operation

---

[27] Buda, Gary, et al. "Security Standards for the Global Information Grid." IEEE. 21 Jan. 2009 <http://http://ieeexplore.ieee.org.leo.lib.unomaha.edu/stamp/stamp.jsp?tp=&arnumber=985877&isnumber=21247>.
[28] "Human Error, Not Software, the Main Cause of Network Failure." ComputerWeekly.com. 17 May 2009 <http://www.computerweekly.com/Articles/2004/02/10/200073/human-error-not-software-the-main-cause-of-network.htm>.
[29] "Human Error, Not Software, the Main Cause of Network Failure." ComputerWeekly.com. 17 May 2009 <http://www.computerweekly.com/Articles/2004/02/10/200073/human-error-not-software-the-main-cause-of-network.htm>.

Enduring Freedom. Here the security measures were in place, but were completely bypassed by a senior officer who wanted to access the Internet. The senior officer "[took] the cabling from the inside router and connected to the Internet for connectivity, thus bypassing all firewall services, encryption, and the entire secure network with a jump straight to the Internet."[30] As previously evidenced, users are a vital but detrimental aspect of the GIG, giving the information and systems meaning and value, but they also cause large amounts of network problems. Recommendations, which will later be discussed in greater detail, include such things as basic system upkeep (e.g., anti-virus, firewalls, regular system health checks, etc.) and user accountability. Users should take it upon themselves to adhere to security protocol by taking responsibility for personal actions, or lack thereof, and defending the network from both internal and external threats. General Chilton, the USSTRATCOM Commander, stated at the 2009 Cyberspace Symposium that "changing culture is absolutely important…" and "there are adversaries out there who are taking advantage of that misbehavior and lack of discipline…" currently found in DoD culture and adherence to security protocol.[31] The necessity for cultural change and user accountability within the DoD along with additional solutions is a necessary factor when determining metrics to measure the health of the GIG.

Measuring the Health of the GIG

It is helpful to utilize an analogy between the GIG computer system and the human body when considering a means to measure GIG health. The World Health Organization (WHO) defines the term health in the preamble to the organization's constitution as "[a] state of complete physical,

[30] Rist, Oliver. "Stupid User Tricks: 11 IT Horror Stories." InfoWorld 13 Apr. 2006. 18 May 2009 <http://www.infoworld.com/d/adventures-in-it/stupid-user-tricks-eleven-it-horror-stories-822>.
[31] Chilton, Kevin P. (2009, April). Opening Remarks. *USSTRATCOM Perspective*. Symposium conducted at the meeting of the 2009 Cyber Symposium, Omaha, Nebraska.

mental, and social well-being and not merely the absence of disease or infirmity."[32] This definition of health is a consistent measure of biological health; likewise, a similar definition can be derived to describe the health of the GIG using such terms as sustainability, reliability, and survivability.

Overall, the framework for metrics to analyze the health of the GIG focuses on sustainability, reliability, and survivability. The GIG can be viewed as very similar to the human body, which is a living, breathing set of many different systems that come together for the single purpose of life. Sustainability can be analogous to the different organ systems within the human form. For example, the circulatory, muscular, or digestive systems have their own specific functions, but in combination with the other various systems within the body, they allow for relatively seamless overall functioning. It is essential to maintain and monitor every component of these systems with regular health checks because the failure of any one organ or system will significantly degrade overall health. Reliability can be analogous to the blood, the electrical impulses within the nervous system, and parts of the immune system. Both blood and electrical impulses carry important messages throughout the body by stimulating the release of certain hormones resulting in particular reactions. This is akin to certain information, perhaps propaganda, resulting in maladaptive feelings towards another entity. The direct electrical impulses carrying the sensitive data could also result in movement (i.e., actions taken with or against that other entity) or thought (i.e., intelligence that gives someone an advantage over another). The immune system is comparable to security measures within networks tasked to defend against malicious actors or alteration of data. Within the human body the malicious actors are viruses or harmful bacteria, but within the GIG, malicious actors could be anything from botnet armies or cyber-terrorists to

[32] World Health Organization. "WHO Definition of Health." Constitution of the World Health Organization: Preamble. 13 May 2009 < http://www.who.int/about/definition/en/print.html>.

a user improperly handling equipment or software. An immune system that is functioning at a normal level on a regular basis prevents attacks that can result in an overall lowering of one's health, the way one feels, and level of performance. Humans can help boost the immune system through regular exercise, eating nutritionally, and getting a full nights rest. Maintaining the GIG's immune system would require similar measures like regular data and equipment trials, keeping a watchful eye on who or what enters and/or uses the system, and ensuring no one part of the system is overworked. Survivability can be analogous to reactive measures taken to ensure the human body (or network) can continue to fulfill its mission in the face of an attack or threat. For example, when a human is involved in a major event, perhaps a car accident (i.e., an attack) the primary concern is preservation of life (i.e., ensuring continued mission fulfillment). Measures are taken to ensure the sustainment of life even if an irreparable part of the system has to be removed. After such an event, there should be ample time to rest and recover. If an attack occurs on the network, the main concern is whether or not the network can continue to fulfill its mission. Anything should be done to ensure the entire system can survive, even if it includes cutting off service or communications to a segment of the network. Another way to understand the measurement of the GIG is to think about a time continuum.

The time continuum includes sustainability, reliability, and survivability and encompasses preemptive measures, data availability and accessibility, and reactive measures over time. Sustainability is the consistent performance of network tasks with focus being on the health of hardware. Upkeep should be a preemptive measure as sustainability concerns the physical health of the system (e.g., hardware and software). Consequently, it is important to recognize beforehand when a device is likely to fail for the following two reasons: (1) services can be rerouted to backup device and (2) a replacement device can be ordered. Reliability is user

accessibility and information integrity with primary focus on data availability and accuracy. Survivability, as it concerns the network's ability to survive an attack, can be viewed as a reactive measure. However, preemptive considerations must be taken into account to ensure that reactions are appropriate and timely.

The human health and time continuum analogies will be discussed more fully as each aspect of GIG health is considered and explained. Metrics for sustainability, reliability, and survivability will be outlined as well as methods for weaving them together to obtain one consistent measurement of GIG health.

SUSTAINABILITY

The first aspect of GIG health is sustainability, which corresponds to physical well-being, the first term mentioned in the WHO health definition. Physical well-being encompasses the strength of the body's muscles, the health of its organs, and its energy and vitality.[33] Physical health implies that the body can complete the daily tasks of life with youthful vigor and that a human's organs are working well, thus indicating that the body has the ability to sustain itself. This definition can be abstracted to apply to the "physical" health of a computer system. Completing daily tasks with youthful vigor relies on the body's muscles, bones, and other somatic aspects. Similarly, a computer system's ability to complete the user's requests depends on strong hardware and software. This means that the individual devices, computers, and servers that make up the GIG are operating effectively and also that software is up-to-date (i.e., healthy). These important aspects of system health are encompassed in the term sustainability. Just as it is important for each organ in a human body to work effectively and perform function on a daily basis, each component of a computer system must also be healthy and perform tasks both efficiently and effectively.

A sustainable network is capable of storing, transporting, and sharing information over a specified interval of time, given expected conditions.[34] In order to accomplish this task, the network's hardware must be fully functional and be able to continue consistent performance in its current environment. A question to be posed when discussing sustainability within a network is "how long will the network continue to perform its mission before inevitable failure?"

---

[33] "physical fitness." Encyclopædia Britannica Online. 1 May 2009 < http://www.britannica.com/EBchecked/topic/458677/physical-fitness>.

[34] Varshney, Upkar, et al. "Measuring the Reliability and Survivability of Infrastructure-oriented Wireless Networks." IEEE (2001) 611-618.

Sustainability assumes protection against extreme, unforeseen circumstances, relying solely on the probability of failure within predictable conditions.[35]

Measuring sustainability across the entire GIG is a complex process, due to the dynamic composition of components and environments within the GIG. Universal factors are not present within the GIG because networks exist within very different environments that perform unique tasks. Two similar pieces of hardware could be expected to perform operations in very different conditions depending upon where they are located. For example, one network router could operate in an air-conditioned office while a similar router could operate outdoors in a hot, sandy environment. Equivalent Central Processing Unit (CPU) systems could be used for the following distinctive functions: one CPU could be used for basic Internet browsing with another as being used as part of a weapons guidance system. The complexity of the GIG makes it difficult to use standard sustainability measurements, but it is feasible to segment the process and use techniques like evaluating operational environment on the individual components within a network.

Sustainability of the network's hardware can be expressed in terms of a probability: how many times has a component failed as compared to the total number of times a specific task has been performed?[36] In this context, a failure does not refer to critical failures but instead refers to uncompleted operations or reported errors during normal functioning. These types of failures do not prevent devices from continuing to operate, but in some cases may prevent a device from completing its mission in a desired time span. For example, if a machine creates 1,000 widgets in an hour, a probability could express how many widgets were completed without any flaws. In

[35] Menard, Philimar. "Reliability vs. Availability: Clearing up misconceptions." Communications Technology. 12 Mar. 2009 <http://www.cable360.net/ct/operations/bestpractices/Reliability-vs-Availability_33189.html>.
[36] Menard, Philimar.

terms of the GIG, sustainability can be expressed in terms of how many network operations are attempted versus how many times these network operations reported failure.

In order to obtain an accurate probability of the network's sustainability, administrators performing a health check should obtain specific details about the components within the network.[37] To assess sustainability, the intended functions of the network or network component should be identified.[38] Knowing if the network has performed its intended functions without failure requires a clear definition of failure and knowledge of what type of actions would constitute a failure.[39] The specific time interval in which an intended function is required to perform should be assessed and provided in units relevant to the part in question.[40] For instance, a warfighter might use two similar devices over the course of two years. However, if the warfighter uses device A hourly and device B monthly, device A might fail significantly sooner because of more frequent use. Therefore, it could be more effective to use a time interval like working hours instead of years to measure a device's desired time interval. Finally, to accurately assess the sustainability of a network, ideal conditions of each network component, such as temperature, moisture, pressure, etc., should be defined in order to assess whether the conditions are being adhered to and compared to the actual conditions of its use.[41] For example, if a particular router is designed to run in cool, dry environments, the sustainability score should reflect if that router is instead being used in a hot, humid environment.

Each individual device (or component) has its own specific function within the network, or its role in contributing to network functionality. This can be illustrated by a hypothetical server that

---

[37] Menard, Philimar. "Reliability vs. Availability: Clearing up misconceptions." Communications Technology. 12 Mar. 2009 <http://www.cable360.net/ct/operations/bestpractices/Reliability-vs-Availability_33189.html>.
[38] Menard, Philimar.
[39] Menard, Philimar.
[40] Menard, Philimar.
[41] Menard, Philimar.

has the task of backing up surveillance data obtained from reconnaissance missions and is scheduled to perform backups every 48 hours. For added redundancy, this server has been designed to backup new files, as well as files already in existence within the backup data. Knowing the server's purpose, backing up surveillance data, makes it possible to assess whether the component is actually performing its intended function. For example, if it is realized the backup server has only been backing up new data, but not already existing data, the device would not be fulfilling its role within the network.

However, determining the specific function of a device or component is not enough. With the high performance technology found in most networks, individual components could have multiple, highly dynamic roles. It could be helpful to know the scope of these roles and how each component can impact the network and the GIG, though this can be an incredibly complex process. The GIG has been described to have "black holes" or areas where specific devices and their functions are unknown. These black holes generally exist for the following two reasons: (1) lack of communications between networks resulting in gaps between an organization's grasp of the available data and resources and (2) strict security measures that stem from a culture of protecting and guarding information rather than sharing it.[42] While it is important to protect information both from external agents seeking to harm the U.S. and internal agents without adequate clearances and a "need to know," these "black holes" could prevent war fighters from obtaining all of the tools necessary for mission success.

Even when a device is known to be in use, the extent of its effect on network performance is largely unknown. Sometimes, the wide scope of a device's contribution to the network is

[42] Chilton, Kevin P. (2009, April). Opening Remarks. *USSTRATCOM Perspective*. Symposium conducted at the meeting of the 2009 Cyber Symposium, Omaha, Nebraska.

unknown until the functioning of that device has failed. For instance, it may be known that the surveillance data backup server is used for storing backup data, but it could be unknown that some areas of the GIG actually pull surveillance data directly from the backup server, rather than the common network server expected to provide such information to the GIG. In this situation, a critical failure of the backup server would affect all areas of the GIG that pull data from the backup server. This example would not be an expected consequence of server failure, but would soon be realized as areas of the network reported an inability to obtain necessary surveillance data. While these situations should be avoided, network administrators could use these failures to log the effects of such events in order to develop a more complete understanding of network functions associated with a particular device.

Identifying the specific function of a network device could also help define the conditions of a failure for that device. For example, if the job of a particular network device is to repeatedly perform a precise calculation, how large should an error be to be understood as a failure of the device? A balance of flexibility and rigidity could be used and would correlate with the criticality of the specific device.[43] If the device in question is essential to mission success, such as a server holding guidance information for warfighters in theatre, more rigid guidelines could be established since even a small error could prove to be critical to the mission. The right balance of failure thresholds is essential for an accurate measurement of sustainability as thresholds with too much flexibility could create an illusion of a network with higher sustainability than actually exists. The opposite problem, using thresholds that are too rigid and not allowing enough room for error, could elicit a high failure rate and a sustainability measurement that is too low, thus creating the illusion of network problems that may not exist.

[43] Menard, Philimar. "Reliability vs. Availability: Clearing up misconceptions." Communications Technology. 12 Mar. 2009 <http://www.cable360.net/ct/operations/bestpractices/Reliability-vs-Availability_33189.html>.

To ensure that correct failure thresholds are being employed, it could be useful to compare observed failure rates of devices within the GIG using a metric known as Mean Time Between Failures (MTBF). MTBF expresses the working life of a given component in statistical terms and is the most common metric used when measuring network sustainability.[44] [45] In relation to the GIG, MTBF could be beneficial in determining the most reliable products, assessing the longevity of devices already in use, or as a baseline failure rate from which to base appropriate parameters of failure. In order to calculate MTBF, a large sample size of matching pieces of equipment is needed and time intervals between failures must be collected in a lab or from the field and averaged together.[46] The large size of the GIG can be helpful in this regard, especially if practices are implemented to obtain and record as much data as possible from equipment failures. With the high volume of devices in use across the GIG, a sufficient sample size would be relatively easy to obtain, enabling MTBF to be used most effectively. On the other hand, measurements obtained from a lab setting could allow for environmental factors to be more precisely controlled to effectively isolate any variables that may have an effect on the failure of a device. Both methods of data collection could be used to provide the greatest MTBF reliability. A wide array of information gathered about environmental conditions during such failures (e.g., ambient temperature, moisture levels, and vibration rates) will increase the reliability of MTBF. Another benefit to using the MTBF metric is its ability to be modified to account for virtually unlimited amounts of factors, especially if the MTBF calculation was automated within the GIG. Using standards from MIL-HBK-217, the Military Handbook for establishing reliability

[44] Kay, Russell. "MTBF." Computer World 31 Oct. 2005: 30.
[45] Varshney, Upkar, et al. "Measuring the Reliability and Survivability of Infrastructure-oriented Wireless Networks." IEEE (2001) 611-618.
[46] Kay, Russell. "MTBF." Computer World 31 Oct. 2005: 30.

guidelines of equipment used within the DoD, a GIG MTBF could include reliability measurements already deemed critical by past DoD research.[47]

However, even with reliable data, MTBF should not be expected to predict exactly when a single device will fail. As a statistical measure, MTBF is most accurate at assessing probabilities of failures across a population of particular pieces of equipment.[48] Therefore, MTBF could be best used to predict vulnerabilities of hardware within the GIG. Essentially, a low MTBF contributes to low sustainability because devices cannot be expected to continue to perform over time without failure. For instance, if it becomes apparent that a specific model of network servers has a low MTBF, then replacing them with similar devices of higher MTBF would increase the sustainability score across the GIG.

MTBF assumes an ability to repair equipment, but for devices that cannot be repaired it could be more effective to use the Mean Time to Failure (MTTF) metric. MTTF can be calculated by measuring the total operating time observed in a device before a critical failure occurs in which the device can no longer be repaired.[49] MTTF can be measured using similar techniques as the MTBF metric, and it can be implemented within the GIG using the same methods as MTBF. Vulnerabilities could be more easily detected in GIG devices by keeping track of equipment being used and factors that could shorten the expected MTTF for a device. MTTF could also be useful in predicting the interval of time a component will perform its intended functions. Information like working hours could be compared to the expected time interval using a standard bathtub curve of component failure (see Figure 2).

---

[47] Air Force. "Military Handbook for Reliability Prediction of Electronic Equipment." Quanterion Solutions Incorporated. 1 May 2009 <http://www.quanterion.com/Publications/MIL-HDBK-217/MIL-HDBK-217F%20w%20N1%20and%20N2.pdf>
[48] Kay, Russell. "MTBF." Computer World 31 Oct. 2005: 30.
[49] Kay, Russell.

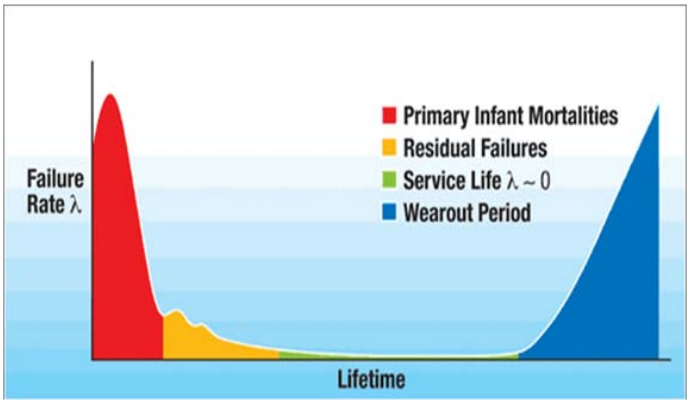

Figure 2: Theoretical Bathtub Curve for Failure Rates[50]

The bathtub curve is a common tool used in assessing product reliability that predicts a component's expected time interval based on its observed failure rates.[51] Figure 2 shows a component's highest expected rate of failures, meaning the least amount of time between failures is during its infant and end of life stages. By observing the slope of failure rates over an interval of time, it can be known in what stage of life a component currently exists. For example, the first stage of a component's life is called the "infant" stage, and is "characterized by a high but rapidly decreasing failure rate."[52] This stage usually lasts for several weeks or a few months. After this initial stage, the failure rate should level off for the majority of the life of the component. The final stage of life of the component is the Wearout Period, which is identified by an increasing failure rate.[53] Knowledge of a component's status on the bathtub curve could help assess the risk of it experiencing a critical failure where it would need to be replaced.

---

[50] Gerstle, Don. "Burn-In Issues." Electronic Design. 17 Apr. 2009 <http://europe.elecdesign.com/Articles/ArticleID/10777/ 10777.html>.
[51] NIST/SEMATECH. "'Bathtub' Curve." Engineering Statistics Handbook. 24 July 2009 <http://itl.nist.gov/div898/handbook/apr/section1/ apr124.htm>.
[52] NIST/SEMATECH.
[53] NIST/SEMATECH. "'Bathtub' Curve." Engineering Statistics Handbook. 24 July 2009 <http://itl.nist.gov/div898/handbook/apr/section1/ apr124.htm>.

Both MTBF and MTTF metrics would be a valuable tool for an assessment of sustainability, and their ease of execution could mean a relatively straightforward implementation into GIG architecture. However, their inability to provide any specific predictions makes it unlikely that these metrics could be used in isolation to provide an accurate picture of network sustainability. Therefore, it would be critical to use MTBF and MTTF together, combining results with information regarding the sustainability of the software used within the GIG in order to provide a more accurate picture of sustainability across the entire system.

A device's MTBF and MTTF may vary depending on the environment in which it is being used. A network router being used in an office setting could have a significantly higher MTBF or MTTF than the same router being used in theater. Therefore, it could be helpful to keep track of key factors within each individual device to provide a more reliable prediction of its expected life span. In order to obtain this information, a self health check could be implemented in which key factors concerning the external environment and the device itself could be measured by both internal and external sensors. Future devices would include environmental sensors within the devices themselves, or current network environmental monitoring devices would be used to measure environmental factors in such areas as wiring closets, server rooms, or any place where a high concentration of critical hardware exists. Measurements used in MTBF calculations could be stored in information databases for accessibility by network administrators, or any authorized personnel interested in a deeper understanding of current GIG hardware health.

A similar method is being researched by the health industry to allow for wireless patient monitoring.[54] In patient monitoring, vital signs of patients are monitored by capable devices and

[54] Varshney, Upkar,et al. "Patient Monitoring Using Ad Hoc Wireless Networks: Reliability and Power Management." IEEE Communications Magazine 2006: 2-8.

routed to interested physicians and nurses wirelessly.[55] Transmission of vital signs can be done periodically, or be designed to alert interested parties in the case of a reading outside of safe parameters. If the GIG is viewed as a living, breathing system, the health care example can be more easily applied to a GIG self health check. For instance, a patient's vital signs, such as heart rate, blood pressure, and temperature could be translated to failure rate, CPU cycles, vibration rates, and external factors like temperature and moisture levels. These factors could be checked periodically, or vital signs of the GIG could be designed to send an alert when a measurement is observed to be outside the range of "safe" conditions.

The Service Oriented Architecture (SOA) of the GIG would allow for the devices themselves to monitor workload factors such as failure rate and CPU cycles. SOA allows for services and applications to be shared across entire organizations, or in the case of the GIG, across an entire network grid. This allows for similar tasks to be performed in the same way using the same programs and programming languages across the entire GIG. Services like error reporting and performance diagnostics could be pulled from the GIG, rather than having to be loaded onto each computer. Using SOA across all GIG systems would create universality of reporting techniques and should allow for greater compatibility to information of a GIG database.

While the self health checks and environmental monitoring would be effective in assessing sustainability, there will likely be scenarios when all factors deemed critical by MIL-HBK-217 have not, or cannot be obtained for a device within the GIG. However, lack of information could also be factored into a sustainability metric or a device's MTBF by multiplying the calculated MTBF by its percentage of necessary information. For example:

*MTBF * (number of factors obtained / number of critical factors) = rMTBF*

[55] Varshney, Upkar, et al.

This simple equation could help to create a reliability score for the metric itself (rMTBF) creating a more complete understanding of the metric's reliability. The procedure could also encourage more complete knowledge of the devices within the GIG as those seeking maximum sustainability scores for their network would seek to increase their rMTBF scores by taking more measurements of equipment.

Risk Analysis and Software Sustainability

According to the National Institute of Standards and Technology (NIST), prediction of vulnerabilities for software "should be able to be drawn from historical data collected about the characteristics of other similar types of software…and the vulnerabilities they experienced."[56] While the metrics used for hardware cannot be directly applied to software, similar principles could be applied to predict the sustainability of GIG software. Much like hardware, software failures could be monitored, reported, and interpreted to better understand causes, risks, and future fixes. Similarly, if a virus is known to attack a particular type of operating system, knowledge of what devices are currently running that system could help to assess how at risk those devices are and how likely it is that they will continue to run normally.

Software sustainability is dependent on different factors than hardware sustainability, and the MTTF and MTBF metrics would be ineffective in assessing the sustainability of the software used. Instead, more advanced risk analysis techniques could determine how much longer the software currently utilized can be expected to ensure mission fulfillment. In technology, it is critical to be up to date with current threats, vulnerabilities, and update potentials to properly assess longevity estimates. According to Stephen R. Melvin, an expert in Risk Management

[56] Jansen, Wayne. "NISTIR 7564: Directions in Security Metrics Research." National Institute of Standards and Technology, 31 Mar. 2009 < http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>.

associated with the U.S. Government, risk is a combination of the likelihood and the severity of an event or scenario.[57] Risk analysis seeks answers to the questions "how likely is this event to happen?" and "what are the consequences of this event?" Two general types of risk assessment exist: qualitative and quantitative. The qualitative approach requires the most subjectivity and expertise of a situation while the quantitative approach is less subjective and uses statistics to obtain a fixed number from which a decision is made. An example of the qualitative approach is when a person decides to drive a car to work because it is believed that it is safe to do so. The decision could be based on having driven the same route before and never having been in an accident or current conditions may not suggest any increased risk of having an accident. Using the quantitative approach, the same driver would have to calculate the risk of an accident using statistics based on current weather, rate of speed, and etcetera before coming to a decision.

Both methods of analysis have strengths and weaknesses. The quantitative approach is fundamentally more objective and therefore would prove to be more reliable over time. However, given the vast size and complexity of the GIG, obtaining fixed numbers and definite statistics may be difficult and would require an accurate modeling of the GIG, which at this time is non-existent. The qualitative approach does not require fixed numbers or definite statistics, but instead relies on experts' knowledge to obtain a score on a sliding scale.[58] This approach could be the most beneficial for the GIG.[59] Experts could pool their knowledge of current risks along with their existing knowledge of GIG networks and software to derive a risk level based on a sliding scale.

[57] Melvin, Stephen R. Personal Interview. 31 Mar. 2009.
[58] Melvin, Stephen R.
[59] Melvin, Stephen R. Personal Interview. 31 Mar. 2009.

However, the complexity of the GIG could make the qualitative process very difficult, and at this point, unrealistic. Also, to perform a qualitative analysis of risk across the GIG would require too much time between the data being gathered and interpreted for any findings to have relevance to current GIG health. Instead, the GIG could benefit from the use of a semi-quantitative approach where panels of experts from different segments of the GIG assign a fixed number (quantitative) to a qualitative scale.[60] Segmenting the GIG could help to alleviate difficulties due to its vast size, and could also allow experts to narrow the focus to allow for a deeper understanding of one specific segment. Assigning fixed numbers to a qualitative scale could allow for a shared understanding of risk across all GIG systems, and using a numerical value could allow risk to be assessed in the global health metric discussed later.

The semi-quantitative approach would benefit from the use of common terminology and definitions. This common "language" would increase the likelihood that risk is being assessed similarly across all GIG segments, and that an analysis conducted for one segment would be directly applied to another segment containing similar software and devices. A standardized method already being used by the U.S. Computer Emergency Readiness Team (US-CERT) is the Common Vulnerability Scoring System (CVSS).[61] This standardized vulnerability scoring system uses a series of metrics, such as exploitability, collateral damage impact, and authentication, to calculate a score (0-10) reflecting the level of vulnerability for any program, device, or service.[62] CVSS is an open service, meaning that any organization can contribute to the scoring system provided they adhere to scoring guidelines and describe how the score was

[60] Melvin, Stephen R.
[61] US-CERT. "Vulnerability Summary for the Week of December 10, 2007." Cyber Security Bulletin SB07-351. 13 May 2009 <http://www.us-cert.gov/cas/bulletins/SB07-351.html>.
[62] Mell, Peter, et al. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." Global Initiatives. 12 May 2009 <http://www.first.org/cvss/cvss-guide.html>.

reached.[63] US-CERT utilizes the scoring system in its weekly vulnerability summary in which products and their vendors are listed along with a description of vulnerabilities and a corresponding CVSS score. A similar approach could be used across all GIG systems by implementing a global database of known vulnerabilities. Vulnerabilities of software being used within the GIG could be indentified within individual networks and reported to the database to allow for shared awareness across all GIG networks.

While the semi-quantitative approach increases the reliability of a risk assessment, the lapsed time could mean that any results from an analysis are irrelevant to the current status of the GIG as new threats may have appeared after the analysis was conducted. Therefore, the semi-quantitative process (or steps of the process) could be automated to allow for real-time analyses of GIG sustainability. Automating key measurements of network devices could help decrease the time required to achieve full situational awareness of current conditions and vulnerabilities of GIG devices. Key measurements obtained through self health checks could be automatically fed into software and hardware sustainability metrics. Here, the numeric value of the sustainability metric would be consistently available and continuously updated as results from health check are reported. By having access to and knowledge of what the metric is saying about the GIG's sustainability, analysts and experts could more rapidly come to conclusions about current GIG health. Results from the sustainability metric could then be combined with scores from reliability and survivability measurements in order to create a more complete picture of overall GIG health.

[63] Mell, Peter, et al. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." Global Initiatives. 12 May 2009 <http://www.first.org/cvss/cvss-guide.html>.

Sustainability: Commercial Best Practices

Sustainability is commonly evaluated in the commercial sector by utilizing a comprehensive framework similar to the self health check method previously detailed. An example is Cisco Systems, which currently uses an architectural approach to security that incorporates a security framework throughout the system and considers the entire Information Technology (IT) lifecycle. Coined the Cisco Security Control Framework, it evaluates the architecture that protects the extended network infrastructure. Cisco also uses a Security Architecture Assessment Service that identifies gaps in the security infrastructure and provides a step-by-step procedure for remedies. The Cisco Security Architecture Assessment Service is similar to the proposed semi-quantitative risk analysis and could be used in the GIG to address vulnerabilities in the system.[64]

Cisco security experts and engineers undergo a detailed process that begins with a review of the company's security goals and needs. Next they begin an in-depth examination of the existing security infrastructure that may cover aspects such as the network topology, network devices, security devices, and application devices. Engineers then address vulnerabilities in the existing system and determine ways to remedy risks and vulnerabilities.[65] The assessment service could be used in GIG networks for hardware that is not adaptable to the proposed self health check. Security experts could assess GIG hardware and provide a score using scoring techniques similar to Cisco's. The assessment service could also help to identify areas of vulnerability that are not currently being assessed by the self health checks. The foundations for this commercial best

[64] Cisco. "Understand and Strengthen Your Organization's Security Architecture." Cisco Security Architecture Assessment Service. 16 May 2009 <http://www.cisco.com/en/US/services/ps2961/ps2952/cisco_saa_ds.pdf>.
[65] Cisco. "Understand and Strengthen Your Organization's Security Architecture." Cisco Security Architecture Assessment Service. 16 May 2009 <http://www.cisco.com/en/US/services/ps2961/ps2952/cisco_saa_ds.pdf>.

practice could be interwoven with the proposed metrics outlined in this section to create a comprehensive measure of GIG sustainability.

RELIABILITY

The second aspect of GIG health is reliability, which corresponds to social well-being (or social intelligence) and is another term mentioned in the WHO health definition. The subject of social intelligence as a part of biological health has been explored by many psychologists. Dr. Philip Vernon, a respected educational psychologist, defined the term as "the ability to get along with people in general… susceptibility to stimuli from other members of a group, as well as insight into the temporary moods or underlying personality traits of strangers."[66] From this definition it can be gleaned that someone who is socially intelligent can read social situations well and respond to other people appropriately. Within this situational awareness comes the ability to detect suspicious persons and protect oneself from manipulation. Equally, a computer system like the GIG must be socially intelligent as it should respond to user requests in a timely and appropriate manner and keep its information accurate and protected from malicious threats. These two aspects of social intelligence—availability and integrity—are important for both human social health and for computer system reliability.

Each day the number of mission critical tasks reliant on the GIG system grows.[67] This means that reliability is becoming increasingly important to users around the world with general expectations that the system will be available when needed. As with anything electronic, this may not always be the case, so careful planning and development should occur to counteract potential issues. There are many factors to consider when defining the term reliability. For instance, a large part of reliability concerns the likelihood that the system successfully completes

[66] Vernon P.E. "Some characteristics of the good judge of personality." Journal of Social Psychology. 4(1933): 42–57.
[67] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.

a user request.[68] This factor is rather broad as it encompasses all ranges of expectations a user may have for the system. Another useful way to look at this aspect of reliability is the absence of failure. While this might seem like a simpler definition, it actually pinpoints the problem of defining reliability—it requires a definition of failure.[69] Failure in the GIG will vary depending on the device being measured as one device not completing a user requested task might be detrimental to a mission objective while another might simply cause a small delay. In any case, reliability can be seen as a measure of assurance that the system will complete a requested task.

In addition, the value of data necessitates the need that data reliability be included in the definition for GIG health. Data reliability exists under the network security scope of Information Assurance (IA). According to the National Information Assurance Handbook, IA is a relatively young field that encompasses "measures that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."[70] The definition covers elements that are outside the scope of this project, one example being confidentiality; however, the definition does include data reliability, which is referred to as integrity.

Even before the advent of the Internet, computer security was a subject of much discussion within the U.S. Government. A 1970 report of the DoD's Defense Science Board Task Force on Computer Security examined security issues of government computer systems. The final conclusions of the report referred to several challenges needing to be met concerning security. The first is the importance of thoughtful system design to provide for inherent computer security.

---

[68] Anderson,T. and Randell, Brian. "System Reliability and Structuring." Computing Systems Reliability. CUP Archive (1979): 1-18.
[69] Anderson, T. and Randell, Brian.
[70] "Information Assurance." National Information Assurance Glossary. Committee on National Security Systems. 5 June 2009 <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.

Other recommendations concern a closed versus open environment, which in 1970 referred to the physical location of these systems as the Internet was not yet a reality.[71]

While some of the conclusions of the 1970 report might seem outdated, there are some universal truths it highlights. For instance, systems administrators need to be one step ahead of the learning curve to ensure that correct security measures are more current than the adversary's abilities. Also the concern of having classified information in an open environment while referring to a different type of open environment (i.e., physically accessible to adversaries as opposed to the Internet) still has much validity.[72] Per the team's discussion with experts at a Roundtable meeting with field experts, the availability of classified information when making quick decisions is certainly important, but also considering what information is truly necessary is an important step in determining what information is an acceptable risk and what information needs to be the most heavily safeguarded.

The 1970s computing requirements and environment differs greatly from today, but similar security issues remain. The advent of the Internet has led to increased security concerns as basic security considerations are not supported in the system design. This has resulted in vulnerabilities that must be continuously patched and worked around.[73] While physical security has typically been addressed to its fullest abilities, personnel and administrative policy could be further developed and enforced as cyber becomes the newest war-fighting domain.

---

[71] Ware, Willis. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." National Institute of Standards and Technology. 20 Apr. 2009 <http://csrc.nist.gov/publications/history/ware70.pdf>.
[72] Ware, Willis.
[73] Talbot, David. "The Internet Is Broken." Technology Review. 24 June 2009 <http://www.technologyreview.com /article/16356/>.

Reliability and Information Assurance

As the need continues to grow for trusted computing systems, IA and its key concepts are valuable approaches to consider. One of the most basic, but common models is the Confidentiality, Integrity, and Availability (CIA) Triad that can be used as a basis for assuring a reliable system.[74]

Confidentiality

Confidentiality prevents unauthorized disclosure of sensitive information. It is the capability to ensure that the necessary level of secrecy is enforced and that information is concealed from unauthorized users.[75] Within the government context, this means protecting information by classification level. While confidentiality is an important issue to the GIG, the monitoring of networks was explicitly excluded from this project by the customer, and thus will not be covered.

Integrity

Integrity prevents unauthorized modification of data, systems, and information, thereby providing assurance of the accuracy of information and systems. If data has integrity, one can be sure that it is an accurate and unchanged representation of the original secure information.[76] While access control lists and other such technologies are widely accepted and in use, there still remains the issue of whether the consumed information is accurate and unmodified.

---

[74] Bhaiji, Yusuf. "Network Security Technologies and Solutions." Network World. 20 Apr. 2009 <http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html>.
[75] Bhaiji, Yusuf.
[76] Bhaiji, Yusuf.

A common type of a security attack is called a Man-In-The-Middle.[77] Here, an intruder intercepts data in transfer and either changes or copies it. This type of attack can happen to both encrypted and unencrypted computer traffic.[78]

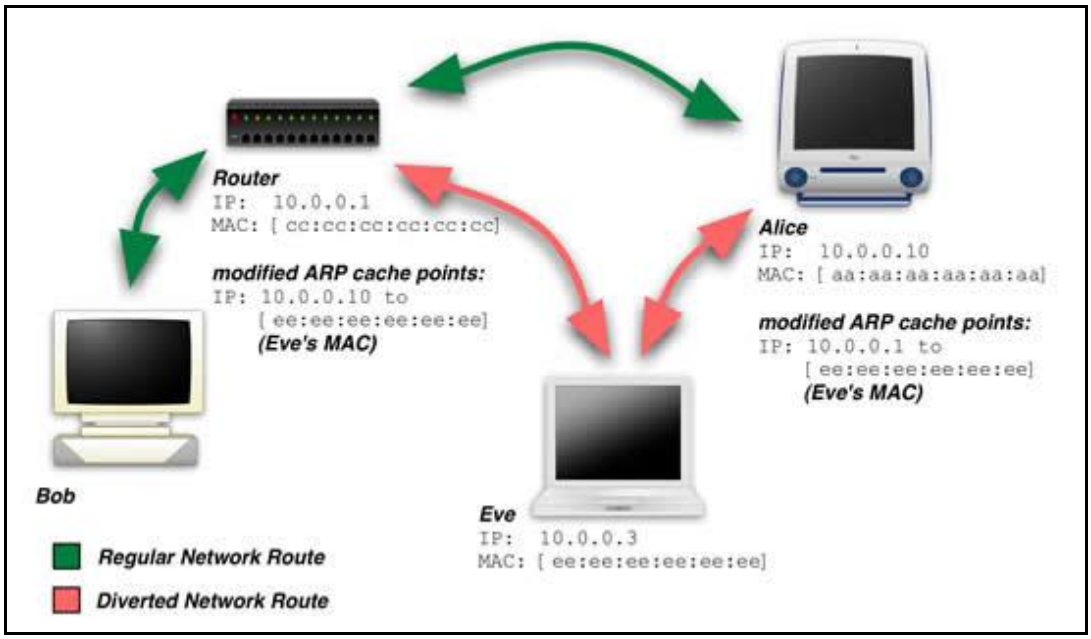

Figure 3: Man-In-The-Middle Attack[79]

In Figure 3, "Eve" is using a program that floods the network with Address Resolution Protocol (ARP) announcements that causes the communication between "Bob" and "Alice" to pass through "Eve."[80] This scenario is considered ARP cache poisoning and is easy to perform on unencrypted text (i.e., human-readable clear-text), but is more challenging on encrypted traffic where the attack typically has to occur at the start of a session.[81] In a Man-In-The-Middle attack, traffic can be intercepted as it passes through a proxy server. The attack occurs between the user's computer and the server hosting the website where all user requests can be forwarded to

[77] Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., 1996.
[78] Schneier, Bruce.
[79] Bittau, Andrea. "WiFi Exposed." Crossroads. 25 Jun. 2009 <http://www.acm.org/crossroads/xrds11-1/wifi.html>.
[80] Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., 1996.
[81] Bittau, Andrea. "WiFi Exposed." Crossroads. 25 Jun. 2009 <http://www.acm.org/crossroads/xrds11-1/wifi.html>.

the attacker who might take or change the data. This includes when a user goes to a HyperText Transfer Protocol over Secure Socket Layer (HTTPS) website where a certificate must be accepted by the user, or on behalf of the user, by the web browser. The proxy server typically changes the Secure Socket Layer (SSL) certificate which encrypts the data during transmission. A warning appears on the browser if something is not right with the certificate; however, most users are willing to bypass the displayed warning and instead continue to the website.[82] In this example, the connection from the end user to the proxy server is encrypted, then decrypted at the proxy server, and re-encrypted as it is sent to the web server. Integrity is compromised because the proxy server is decrypting the traffic and can easily copy or modify the information being transmitted.[83]

One solution to the integrity problem is the use of digital checksums.[84] A checksum is a unique value that summarizes a digital file. More specifically, a checksum is a unique fixed length value which is the result of a hashing algorithm that takes a variable length of data as input. Examples of popular algorithms in use today are Message-Digest algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).[85] An example use of checksums is if a website where files are downloaded posts a link to download both the file and the checksum result. Then the end user downloads the file, runs the downloaded file through a checksum generator, and can be assured the file has not been modified if the checksum matches what was posted on the website. This is one example of verifying that data is not being modified in transit.

---

[82] Bittau, Andrea. "WiFi Exposed." Crossroads. 25 Jun. 2009 <http://www.acm.org/crossroads/xrds11-1/wifi.html>.
[83] Bittau, Andrea.
[84] "Availability and description of the File Checksum Integrity Verifier utility." Microsoft Help and Support. 14 May 2009 <http://support.microsoft.com/kb/841290>.
[85] "Availability and description of the File Checksum Integrity Verifier utility."

Availability

According to Yusuf Bhaiji's article in Network World, "Availability is the prevention of loss of access to resources and information to ensure that information is available for use when needed."[86] Bhaiji communicated that requested information should always be readily accessible to authorized users.[87]

The Internet, as it functions today on the Transmission Control Protocol /Internet Protocol (TCP/IP) was designed to be a network of unreliable networks to provide multiple paths to a specific destination. The Internet standard that was derived from the Internet Protocol Technical Request for Comments (RFC) 791 states, "There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The Internet protocol can capitalize on the services of its supporting networks to provide various types and qualities of service."[88] In addition to that fact, data is transferred in a greedy manner, meaning the Internet will attempt to transfer it as quickly as the network will allow. This is the way many initial Internet Protocols (IP) and services were built as the initial developers of the Internet never planned for a malicious user.[89]

A denial-of-service attack (DoS attack) is an attempt to deny computer resources to intended users, often for the sake of disruption of service. Cyber extortionists have perfected denial-of-service attacks in which thousands of bots are directed to bombard a targeted website with nuisance requests, effectively preventing anyone else from connecting to the site. This can be

[86] Bhaiji, Yusuf. "Network Security Technologies and Solutions." Network World. 20 Apr. 2009 <http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html>.
[87] Bhaiji, Yusuf.
[88] Information Sciences Institute, University of Southern California. "Internet Protocol: DARPA Internet Program Protocol Specification." RFC: 791. 20 Apr. 2009 <http://tools.ietf.org/html/rfc791>.
[89] Talbot, David. "The Internet Is Broken." Technology Review. 24 June 2009 <http://www.technologyreview.com /article/16356/>.

accomplished fairly inexpensively. For instance, a network of several thousand compromised personal computers (PC) can be leased for $1,000 to $2,000 a day. Thus someone can lease a botnet from a bot-herder who advertises online and effectively take down a business for the day. This feat is made easier by targeting businesses unwilling to spend $30,000 to $60,000 for protection.[90] Thus it can be stated that DoS attacks greatly impact system availability and can affect a wide range of websites. As such, it is necessary that proper safeguards and policies be in place to deal with potential issues and downtime.

Traffic management that utilizes Quality of Service (QoS) is one possible solution to offset attacks that deny services. QoS is a term used in packet-switched networks that implement resource reservation and prioritization based on traffic type. Controlling network traffic requires limiting bandwidth to certain applications, guaranteeing minimum bandwidth to others, and marking traffic with high or low priorities.[91] This ability to manage network traffic is vital for services like Voice over IP (VoIP) and media streaming where a network delay can have adverse effects on service performance. The main feature of QoS is packet scheduling, which is the reordering of the output queue of network packets. A simple approach called the priority scheme orders packets by priority and launches the highest priority packets first. The priority scheme has the effect of giving some packets absolute preference over others. In fact, the lower priority class will not be sent if there are enough higher priority packets.[92] This basic example demonstrates issues involved with solving potential denial of service.

---

[90]Acohido, Byron and Swartz, Jon. "Botnets can be used to blackmail targeted sites." USA Today. 17 Mar. 2009. <http://74.125.95.132/search?q=cache:fck5veGX_HEJ:www.usatoday.com/tech/news/computersecurity/2008-03-16-bot-side_N.htm+%22Botnets+can+be+used+to+blackmail+targeted+sites%22+%26+Swartz&hl=en&gl=us&strip=1>.

[91]Klein, Jay. "The ABCs of Traffic Management." CommunicationsNews. 30 Apr. 2009 <http://www.comnews.com /features/2008_july/0708_beyond_testing.aspx>.

[92]Braden, R., Clark, D., and Shenker, S. Integrated Services in the Internet Architecture: an Overview. Internet Engineering Task Force Documents. 30 Apr. 2009 <http://tools.ietf.org/html/rfc1633>.

Proposed Health Metrics

After extensive research, the team concluded that bandwidth usage, diagnostic queries, packet loss or delay, and digital checksums were principal metrics in measuring GIG reliability. Bandwidth usage measures consumed and available capacity within a network or multiple networks. [93] As such, this metric is typically already measured, but is not always monitored or used. Bandwidth usage provides raw data that can be used by the proposed framework; this data provides a general trend of typical use if monitored over time. When usage goes outside the standard deviation of the average, either momentarily or over certain periods of time, the framework could warn of potential issues or attacks that are taking place on a certain network segment.[94]

A diagnostic query could facilitate measuring the reliability of information a query returns. The primary concept of the diagnostic query is to search or request information while measuring the accuracy and timeliness of the response against a known or expected answer. This can provide assurance that requested information is relevant to what is needed. An example would be a search for information regarding a specific region, such as Northern Europe, where a query would be sent for information, and the results would be compared with already obtained results from an earlier search. Because of the dynamic nature of the GIG, the results of a query would change often, but by repeating a diagnostic query, enough information could be logged to obtain a good measurement of system reliability. If the results deviated from what was expected, then the reliability of the system could be regarded as compromised.

---

[93] Prasad, R. S., et al. "Bandwidth Estimation: Metrics, Measurement Techniques, and Tools." College of Computing Georgia Tech. 26 June 2009 <http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/Papers/NetDov0248.pdf>.
[94] Prasad, R. S., et al.

Packet loss and/or delay typically measures or logs data and could be useful in reporting system or service reliability. There are numerous reasons why packet loss occurs: insufficient bandwidth, network connection problems, hardware failure, routing problems, router configuration, and others.[95] If core network routers or switches are experiencing higher-than-normal levels of loss and/or delay, reports could be automatically generated that report to a central management server on the network that feeds into the health framework. There could also be independent ping tests that report round-time response times reporting delay and potentially down systems or services.

The checksum, or unique value that summarizes a digital file, is one of a small number of metrics that could be used to measure data integrity. More specifically, a checksum is a unique fixed length value which is the result of a hashing algorithm that takes a variable length of data as input. Checksums are used to show if data has been modified because if even a single bit in a digital file changes, the checksum would change. Examples of popular hashing algorithms in use today are MD5 (Message-Digest algorithm 5) and SHA-1 (Secure Hash Algorithm 1).[96] Microsoft offers a free download that creates and validates checksums. The File Checksum Integrity Verifier (FCIV) utility can generate MD5 or SHA-1 hash values for files to compare the values against a known value that is good. FCIV can compare hash values to ensure that files have not been changed.[97] This tool can provide the basics to validate files and create a baseline of all checksums for the files on a computer.

---

[95] "Packet loss or latency at intermediate hops." Nessoft Knowledge Base. Nessoft. 14 May 2009 <http://www.nessoft.com/kb/24>.

[96] "Availability and description of the File Checksum Integrity Verifier utility." Microsoft Help and Support. 14 May 2009 <http://support.microsoft.com/kb/841290>.

[97] "Availability and description of the File Checksum Integrity Verifier utility." Microsoft Help and Support. 14 May 2009 <http://support.microsoft.com/kb/841290>.

Reliability: Commercial Best Practices

Networks on college campus are similar to the GIG both in the variety of devices and software that must be adapted to the system and in the assortment of skill level of users who utilize the network. Commercial best practices like WhatsUp Gold and SonicWALL Aventail E-Class Secure Sockets Layer (SSL) Virtual Private Networks (VPN) are valid options to consider when creating a comprehensive measure of GIG reliability.

WhatsUp Gold network management software uses reliability metrics, such as bandwidth usage as well as general network trends like packet loss and/or delay. This commercial best practice example is utilized on the University of Nebraska-Omaha's campus.[98] .

W hatsUp Gold is a web-based application that permits users to login and view the overall status of all computer systems at the university. WhatsUp Gold utilizes bandwidth usage and general network trends (e.g., packet loss and/or delay) to keep a current record of how the network is performing. Figure 4 depicts the initial "heads up display" that provides general information, such as subsystems' status, down services, counts of all systems monitored, and a device listing by type. The user has the option to click on each item for more detailed information.[99]

[98] "Using Ipswitch WhatsUp Gold v12.4." University of Nebraska at Omaha. 26 June 2009 <https://whatsup.unomaha.edu/NmConsole/Help/1033/index.htm?Browser_Check.htm?toc.htm>.
[99] "Using Ipswitch WhatsUp Gold v12.4." University of Nebraska at Omaha. 26 June 2009 <https://whatsup.unomaha.edu/NmConsole/Help/1033/index.htm?Browser_Check.htm?toc.htm>.

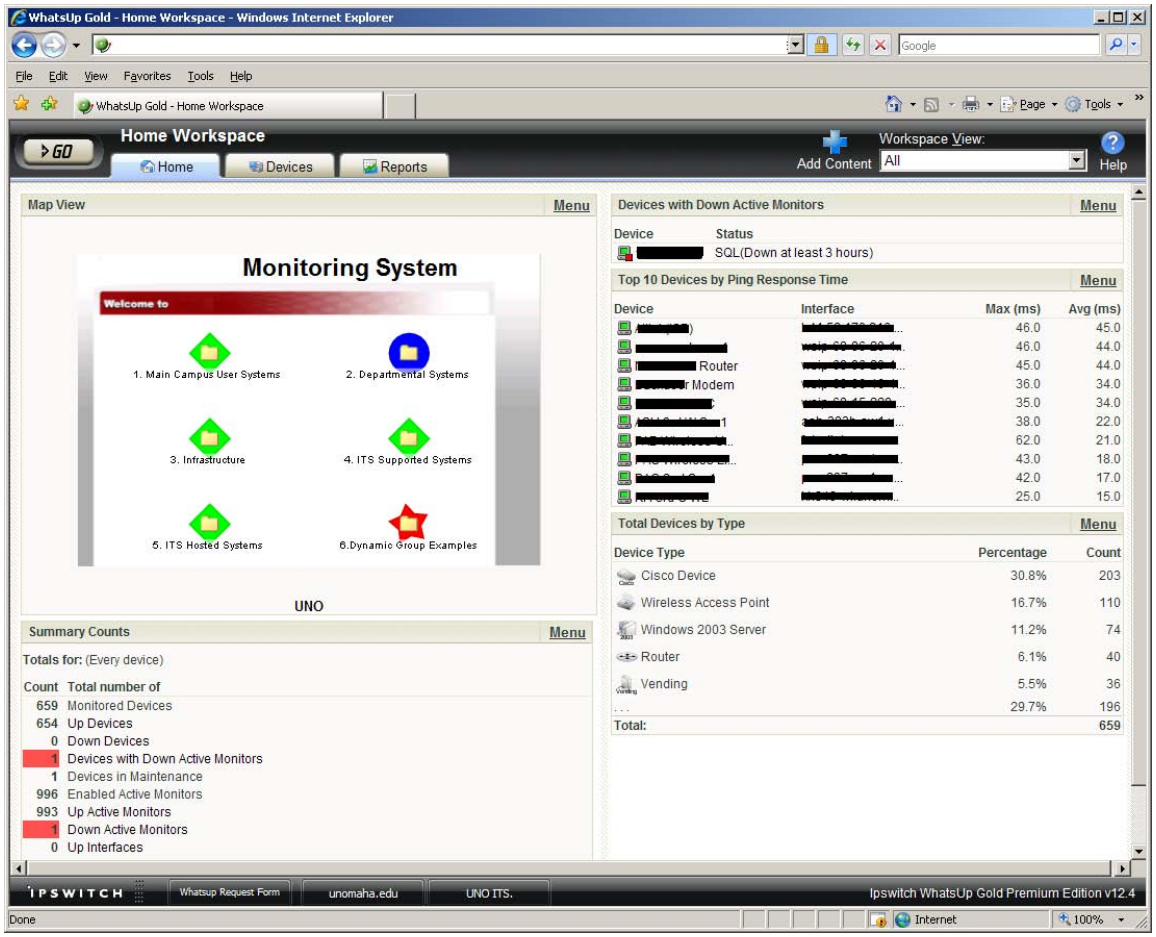

Figure 4: WhatsUp Gold Screenshot[100]

The user may also review data such as departmental information, which is independently operated and maintained, but still managed by the campus-wide technology lead in a directory-like structure. The systems that the department deems critical are maintained in the inventory. Rich information is maintained about each system, including IP address, contact names and numbers, operating system, and other useful information, as shown in Figure 5.[101]

[100] "WhatsUpGold." University of Nebraska at Omaha. 14 May 2009 <http://whatsup.unomaha.edu>.
[101] "Using Ipswitch WhatsUp Gold v12.4." University of Nebraska at Omaha. 26 June 2009 <https://whatsup.unomaha.edu/NmConsole/Help/1033/index.htm?Browser_Check.htm?toc.htm>.

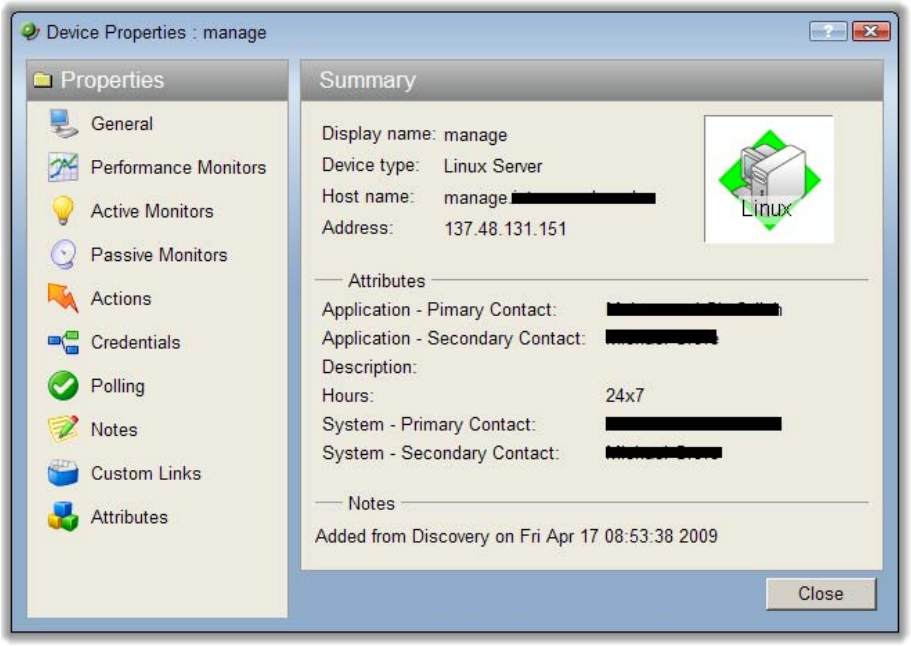

Figure 5: Individual Device Properties Screenshot [102]

To aid in monitoring, alerts can be setup for each device or group. Once certain conditions are met, such as a service not responding for more than five minutes, the system can email, text, or page the appropriate people to investigate the issue.

In conjunction with the in-depth information that is maintained about all critical systems, reporting is another key feature of WhatsUp Gold. Reporting is broken up into seven categories:

1. System – Views logs and diagnostic data for all devices
2. Group – Compares availability and performance data for devices within a selected group
3. Device – Focuses on availability and performance data for a selected device
4. Performance – Focuses on performance data for a selected device or group
5. Problem Areas – Views alerts reported across entire network and troubleshoot problems
6. General – Views workspaces and WhatsUp Gold application logs

[102] "WhatsUpGold." University of Nebraska at Omaha. 14 May 2009 <http://whatsup.unomaha.edu>.

7. Favorites – Custom reports that are frequently used

The user has the ability to detect issues in near real-time and review trends over time. The inventory aspect of WhatsUp Gold is also valuable to detail how many key systems there are in the network, and it provides a great general view to the central IT management.[103]

Another commercial best practice for measuring reliability is the Secure Sockets Layer (SSL) technology used at DePaul University. Modifications needed to occur at DePaul University when the campus decided to accommodate wireless connections for its faculty and 23,000 students over an extensive campus. [104] Originally, the university used Wired Equivalent Privacy (WEP) authentication for on-campus use; however, when this no longer worked appropriately, the university sought an alternative to add to its existing systems. The winner was SSL Virtual Private Networks (VPN) as it could be used with a standard web browser and did not require specific software on the end user's computer. [105] More specifically, the university chose the SonicWALL Aventail E-Class SSL VPN.[106]

Verisign describes their SSL service as having three main ways to secure information. The first is to encrypt sensitive information during an online transaction. This institutes a private communication channel for the information and provides encryption while it is being transmitted. The SSL certificate has a public key and a private key. The purpose of the public key is to encrypt information while the private key is used to decode it. Secondly, each SSL Certificate contains authenticated information about the certificate owner. Each SSL Certificate

---

[103] "Using Ipswitch WhatsUp Gold v12.4." University of Nebraska at Omaha. 26 June 2009 <https://whatsup.unomaha.edu/NmConsole/Help/1033/index.htm?Browser_Check.htm?toc.htm>.
[104] "The Wisdom of Simple Security." CommunicationsNews. 31 Mar 09. <http://www.comnews.com/features /2008_September/0908_coverstory.aspx>.
[105] "Secure Socket Layer Virtual Private Network." Bitpipe.com. 25 May 2009 <http://www.bitpipe.com/tlist/SSL-VPN.html>.
[106] "The Wisdom of Simple Security." CommunicationsNews. 31 Mar 09. <http://www.comnews.com/features /2008_September/0908_coverstory.aspx>.

is set up for a particular server within a specific domain. Lastly, the Certificate Authority verifies the identity of the certificate owner when it is issued.[107]

In addition, SonicWALL emphasizes that, in the modern world of Wi-Fi and other remote technologies and disaster preparation, secure remote access is crucial to the success of any business. A system like Aventail E-Class SSL VPN can make it easier for not only the user, but also for the administrator.[108]

[107] "Secure Socket Layer (SSL): How It Works." VeriSign. 30 Apr. 2009 <http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/index.html>.
[108] "E-Class Solutions: Affordable Enterprise Performance." SonicWALL, Inc. 16 May 2009 <http://www.sonicwall.com/us/products/7523.html>.

SURVIVABILITY

The third aspect of GIG health is survivability, which corresponds to mental well-being and is mentioned by the WHO health definition. According to the Encyclopedia Britannica, mental well-being represents "the prevention of mental disorder, reduction of tension in a stressful world, and attainment of a state of well-being in which the individual functions at a level consistent with his or her mental potential."[109] Mental well-being is relative to the specific person and circumstances that the person is under. Extrapolating the idea of mental well-being to a computer system implies the computer system can respond to a variety of situations. The system must be able to survive under adverse conditions, such as a network failure or attack, just as a human body must be able to withstand both physical and emotional trials during its life span. The well-being aspect of system health is summed up by the term survivability.

Large scale, highly distributed network systems can improve both the efficiency and effectiveness of organizations. However, such a system also presents "elevated risks of intrusion and compromise." [110] To minimize these risks and permit contemporary networks like the GIG to continue working effectively even when compromised, network creators should consider survivability capabilities.

Defining what constitutes the survivability of the GIG is central to determining the ability to measure system survivability with reliable metrics. A study done by R.J. Ellison et al at the Software Engineering Institute defined survivability as "the capability of a system to fulfill its

[109] "mental hygiene." Encyclopædia Britannica. 1 May. 2009 <http://www.britannica.com/EBchecked/topic/375371/mental-hygiene>.
[110] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.

mission, in a timely manner, in the presence of attacks, failures, or accidents."[111] This definition focuses on the internal success of system components and considers external agents (e.g., malware and botnets that could compromise GIG integrity.

In addition to providing a definition for system sustainability, R.J. Ellison et al clarify five key terms regarding the benefits of survivability: mission, fulfill its mission, attacks, failures, and accidents. The authors note the term *mission* refers not only to military objectives, but also to any civil or commercial purpose. In addition, *to fulfill its mission* depends upon the original objective as well as the system's response to external stimuli such as cyber attacks and system malfunctions.[112] *Attacks* are "potentially damaging events orchestrated by an intelligent adversary" and include intrusions and denial-of-service.[113] For this reason a system's survivability should also take into account whether it assumes a defensive or offensive position during an attack, as diverting resources could create new vulnerabilities. *Failures* are "potentially damaging events caused by deficiencies in the system or in an external element on which the system depends… [such as] software design errors, … or corrupted data."[114] Finally, *Accidents* focus more on external events, such as natural disasters or physical events. When assessing sustainability metrics, the combination of more than one of these key terms is necessary to better assessing overall GIG health. For instance, a metric that considers only attacks would not provide a complete and accurate picture of the cyber threats the GIG must be prepared to defend against, and thus could not measure the overall health.

[111] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.
[112] Ellison, R. J., et al.
[113] Ellison, R. J., et al.
[114] Ellison, R. J., et al.

Suppose an attack on a domestic satellite temporarily shuts down communication such that active military personnel no longer have access to the GIG. If the GIG maintains the integrity and confidentiality of all contained data and resumes its essential services when the system goes back on line, the system can be reasonably judged to fulfill its mission.[115] However, if the system randomly shuts down, denying access to users in a time of crisis, it can be said to have failed its mission even if it maintained data confidentiality.

The team used the survivability definition derived by R.J. Ellison et al; however, this is not the only accepted definition. In a 2004 analysis of survivability literature, Dr. Vickie R. Westmark uncovered more than 4,000 publications focused on survivability with 53 distinct definitions of the word survivability.[116] Appendix A contains the 18 definitions that Westmark describes further in "A Definition for Information System Survivability." Many of these definitions would not be sufficient for this analyses herein because it is important to not only have a consistent, strong definition of survivability, but also a definition which can be readily applied to real world networks such as the GIG to better assess the health of the system. Westmark found that "less than 1% of the articles originally selected for potential support to the research area of computational system survivability actually compute survivability."[117] The reports that did compute survivability used "informal calculations… not currently used in practice."[118] Applied reports such as this paper should not make the same mistake. Just as in the work of Cankaya and Nair, computer scientists at Southern Methodist University, the team's survivability analysis and measurement of the overall health of the GIG must provide "quantitative measures for the

[115] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.
[116] Westmark, V. R. "A Definition for Information System Survivability." Proceedings of the 37th Hawaii International Conference on System Sciences. 5 May 2009 <http://www2.computer.org/plugins/dl/pdf/proceedings/hicss/2004/2056/09/205690303a.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253A72.166.249.2 >.
[117] Westmark, V. R.
[118] Westmark, V. R.

network's capability to tolerate failures and to provide continuous service."[119] Overall, "mission fulfillment must survive, not any portion or component of the system."[120]

The composition of the system is also an important element for a survivability analysis. A bounded system can be entirely controlled by a unified administration. An unbounded system, however, combines separate bounded systems as separate wholes without unified control. See Figure 6.[121] It is this unbounded approach that best clarifies the horizontal layered approach of the GIG, as explained in the introduction. There is no one administrative central command to the GIG. Instead, individual systems combine into a cohesive, efficient whole that provides access to up-to-date information to users worldwide.

This great access to information within the GIG comes with a price: greater access for hackers and cyber threats looking for open portals in which to transmit malware into the system, which could lead to a "catastrophic failure."[122] In addition, an unbounded system cannot generally be partitioned into a finite number of bounded environments.[123] This is a great benefit for its adaptability but a weakness when under attack. If a cyber threat emerges from malware on a thumb drive used by an authenticated, authorized user, the threat can spread across multiple GIG domains impacting not only the interface accessed by the user but also all inter-connected interfaces.[124] The result is a system with high user accessibility, but severe risks of mission failure in the face of cyber threats.

---

[119] Cankaya, H.C., and Nair, V.S.S., "A survivability assessment tool for restorable networks." IEEE (2000): 319-324.
[120] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.
[121] Ellison, R.J., et al.
[122] Sullivan, K., et al. "Information Survivability Control Systems." University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.
[123] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.
[124] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.

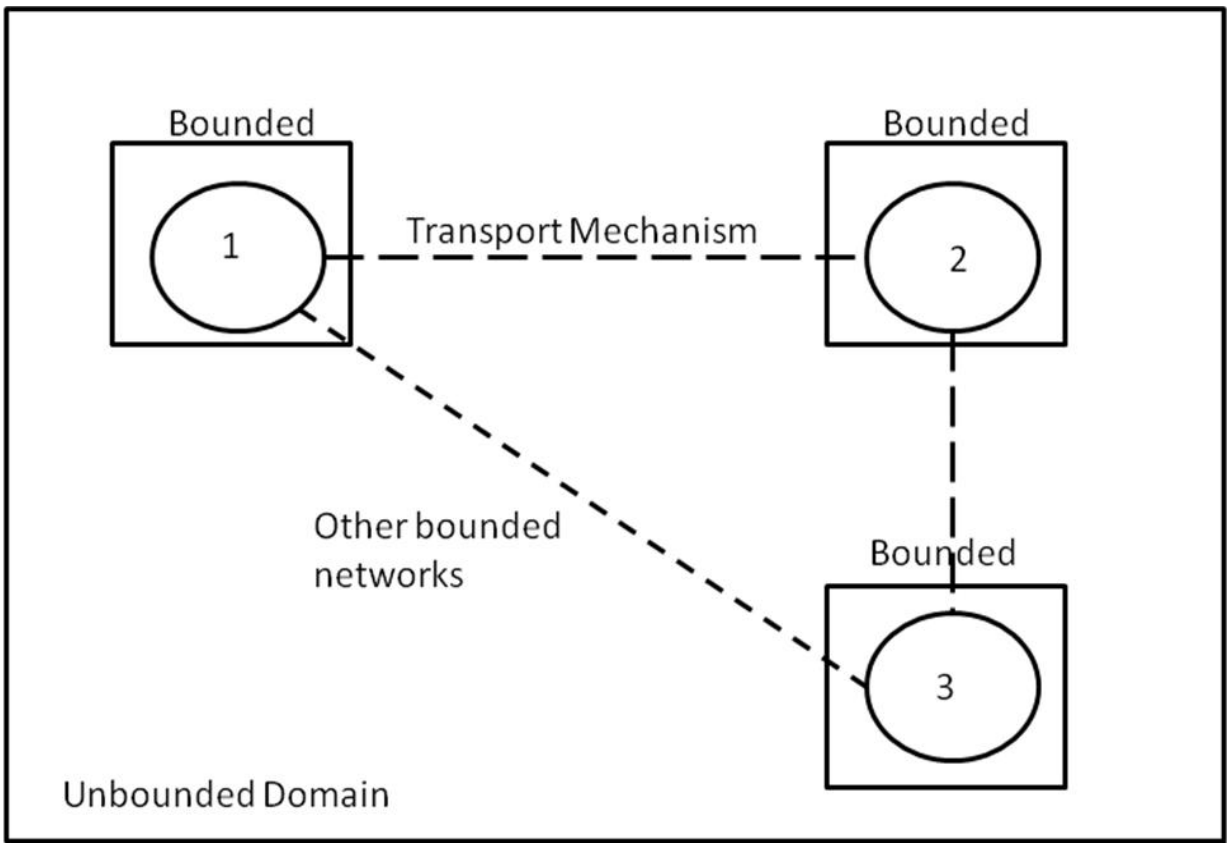

Figure 6: Bounded and Unbounded Networks [125]

The GIG contains specialized networks of classified information that warrants a higher level of integrity and confidentiality than other networks. In addition, the GIG's warfighting mission could not be fulfilled if soldiers in war zones were unable to access the network information, as this would be a major detriment to the system's effectiveness.

Kazman and colleagues of the Software Engineering Institute analyzed multiple attributes of system quality and determined that security attributes traditionally involve availability, integrity, and confidentiality.[126] These attributes should be considered alongside the essential functions of

125 Ellison, R.J., et al.
[126] Kazman, R., et al. "The Architecture Tradeoff Analysis Method." Software Engineering Institute. 9 Mar. 2009

the system which must be maintained for mission fulfillment. For example, if the essential service is the delivery of information to government personnel, this could be achieved by the GIG and also by alternate Internet and telecommunication capabilities. Ellison and colleagues proposed four different major elements required for a survivable system.[127] These elements correspond well to the notions of sustainability and reliability and will be briefly described in reference to a survivability analysis of the GIG.

The first element focuses upon resistance to attacks. Strategies are highlighted to repel attacks and prevent threats from interfering with mission success. Ellison and colleagues suggest that user authentication protocols could create increased security protection and prevent cyber threats and unauthorized users from gaining access to the GIG.[128] In addition, the layered system of the GIG also creates difficulties for those seeking information. Unauthorized access into one area of the GIG can be closed off and limited so that the cyber actor does not gain entry into other unauthorized areas.

The second element focuses upon the recognition of attacks and the extent of any damages. Strategies to understand the current state of the system include damage evaluation in the face of recent and ongoing threats and measures of baseline performance so that, when intrusion does occur, there can be quick recognition of intrusion usage patterns to determine *how much* information was obtained. This also corresponds with the diagnostic query suggestion in the Reliability section. If GIG programs run diagnostic queries to obtain baseline measures of different systems and metrics such as bandwidth spikes, when these measures differ by more than a standard deviation from the baseline, the GIG operators can explore the reason for these

---

<http://www.sei.cmu.edu/architecture/start/publications/atam.cfm >.
[127] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.
[128] Ellison, R.J., et al.

inconsistencies. A quick, computerized alert system will allow continual monitoring of system integrity and appropriate usage to assure a protection system to allow for mission success.

The third element corresponds to recovery of all essential services *after* an attack.[129] Strategies to restore compromised information or functions, limit the extent of damage, maintain functioning, or restore essential services efficiently must occur within the needed time constraints. A rarely used application hidden away into a subfolder on a GIG server might not need immediate restoration, but a folder containing weapons secrets could devastate national security if it became unprotected after an attack. Thus, a swift and efficient recovery is necessary for mission fulfillment and assured confidentiality of classified information. Security measures such as encrypted data and back-up servers to restore activity efficiently and effectively can help restore system integrity in as short a time as possible.

The fourth and final element involves the adaptation and evolution of the system to reduce effectiveness of future attacks. This future-based element seeks to not only respond to attacks but also to prevent them. Strategies to improve system survivability in this element must focus upon gaining knowledge from intrusions and attacks—both in how the attack occurred, what information lost protection, and how the system responded. It is essential for GIG operators to recognize past attacks and malfunctions to adapt the system and meet current security and functional needs.

[129] Ellison, R.J., et al. "Survivable Network Systems: An Emerging Discipline." CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.

Time as a Survivability Metric

Researchers at the University of Luxembourg have posited in the Safeguard project that the time taken to breach a system can be used to measure survivability.[130] This project aims to build demonstrations of survivability in electricity and telecom but the lessons learned can be readily applied to the GIG.

The Safeguard project created a model system where critical service level is expressed as a function of Simulated Machines (SM) which, more or less, tracks whether the critical service level is maintained within the system.[131] In addition, the network receives packets of data that can be classified as either *good packets* or *bad packets*. When bad packets enter a vulnerable network, machines can become compromised and the mission might fail if the bad packet reaches its target within a certain time interval. So how can the interval be estimated? Whenever a system is breached, monitors (automated or manual) can analyze how long it took for a bad packet, botnet, or malware to enter the system and reach a critical component that hinders mission success. Then, these numbers can be utilized as a baseline to track future performance and create new measures which extend the amount of time it takes to compromise the system.[132]

In an experiment within Safeguard, bad packets were submitted into a system. Not only did an observer track the time from entrance into the system to compromise, it also measured the duration from the start of the experiment to when there was a "breakdown of the system."[133]

---

[130] Burbeck, K., et al. "Time as a Metric for Defence in Survivable Networks."Computer Science at the University of Virginia. 15 Mar. 2009 < http://www.cs.virginia.edu/~zaher/rtss-wip/19.pdf >.
[131] Burbeck, K., et al.
[132] Burbeck, K., et al.
[133] Burbeck, K., et al. "Time as a Metric for Defence in Survivable Networks."Computer Science at the University of Virginia. 15 Mar. 2009 < http://www.cs.virginia.edu/~zaher/rtss-wip/19.pdf >.

The GIG, of course, is a large unbounded network that is much more complex than the telecomm network used in the study. However, metrics such as time can be effectively utilized if an automated control console operator works within a control system approach to measure and maintain survivability.

Survivable Systems and Control Theory

The "intuitive notion of survivability is clear: we want infrastructure systems that continue to provide acceptable service levels to customers in the face of disturbances, natural, accidental or malicious."[134] Important to this definition is recognizing the accidental and natural nature of disturbances, which differ from malicious actions. A tornado hitting a facility where information is not effectively backed up could be just as detrimental to system survivability and the overall health of the system as a cyber threat.

Sullivan and his colleagues at the University of Virginia Computer Science Department believe that a control systems approach is best for assessing system survivability. They note that "controlled systems change… so a control system must be adaptive."[135] While this approach focuses upon critical infrastructure systems like those involving electricity, telecommunications, freight, and banking, it can also be used for the GIG. Just as an electric grid provides a stream of electricity that has value and utility to customers, and is catered to their particular needs, the GIG provides a stream of information to war fighters and analysts across the globe. In addition,

[134] Sullivan, K., et al. "Information Survivability Control Systems." University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.
[135] Sullivan, K., et al.

systems such as the GIG or electric grid also provide a "value added" component that stems from the reliance on the network.[136] This added value must be maintained within survivable systems.

The control system perspective of survivability focuses upon continued adjustment and reconfiguration of the system. This reconfiguration is possible "at many levels including operating parameters, module implementations, code location, replacement of physical devices, etc."[137] This is a dynamic approach, where an informational system can create new configurations based upon cyber attacks and ongoing concerns regarding reliability and sustainability in order to maximize the chance of mission fulfillment. Individual components of the GIG can be placed into a type of system hibernation to maximize overall system effectiveness while also minimizing financial costs. In addition, closing off unused portals and system components would also minimize the risks associated with cyber threats entering the systems through these unmanned gates.

A survivable control system should also take into account "sensor data that reflect its state, degrees of control available to the control system" and estimates of future performance indices.[138] In this manner, survivability and sustainability go hand in hand, as assessing how the system works over time (sustainability) can lead to pre-emptive approaches to maintaining survivability in the control system. In particular, after speaking to subject matter experts it has been determined that an *adaptive* control system is best for the GIG. An example of an adaptive control system provided by Sullivan and colleagues is one where an "aircraft remains under control even if it loses part of a wing."[139] This would be effective for the GIG, where the entire

[136] Sullivan, K., et al. "Information Survivability Control Systems." University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.
[137] Sullivan, K., et al.
[138] Sullivan, K., et al.
[139] Sullivan, K., et al. "Information Survivability Control Systems." University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.

system must remain effective to achieve mission objectives even if parts of the GIG go down, whether through cyber threat or natural problems. For this type of system to be effective, GIG architects must create an adaptive control system superimposed upon the current GIG, able to "implement intrusion monitoring and response; system-wide fault tolerance; and controlled service degradation under adverse conditions."[140]

However, empirical research measuring such a controlled system and comparing it to metrics regarding sustainability, reliability, and survivability is limited as researchers' access to systems such as the GIG poses a "serious impediment."[141] Thus, as Sullivan and colleagues suggest, researchers must build operational models that can be compared to the current systems in order to better understand whether the simulation effectively mimics the actual system. This is routinely done in the electric power industry and the lessons can be readily applied to a computer network such as the GIG.[142]

While not a metric *per se* to measure the health of the system, Sullivan and colleagues utilize a Virtual Message Processor (VMP), which is "a flexible mechanism for building distributed dynamic models and control systems."[143] The VMP works as a communication device that dispatches messages to support different mission objectives throughout the system. VMPs also communicate with each other through integer addresses at a network-level.

So what does the VMP system offer for the survivability and health of the GIG? The VMP is an adaptive process where new nodes can be adapted and introduced into the system based upon changing architecture and mission objectives of the entire system. Messages pass quickly

[140] Sullivan, K., et al.
[141] Sullivan, K., et al.
[142] Sullivan, K., et al.
[143] Sullivan, K., et al.

between application nodes, creating a dynamic environment that takes into account both past experiences within the network and also up-to-date changes in response to either cyber threats or internal issues. Sullivan and colleagues explain the use of the VMP system in a banking context with each bank as a node connected to other associated nodes and mediating nodes in between.[144] This, like the GIG, is a hierarchical system, where branch banks are at the lowest level, money-center banks in the middle, and the Federal Reserve at the highest level. The same VMP hierarchical approach could be readily applied to the GIG, as separate structures within the GIG (e.g. SIPRNet, NIPRNet) could be associated through nodes where messages can alert the system of any disruption and maintain mission objectives, including protecting classified information required for the success of the mission and national security. Shell messages can also simulate failures to track how survivable the system is in the face of such attacks.[145] This type of mock attack could be highly informative to understanding the survivability of the GIG and affiliated networks. Overall, the control system employing VMP technology looks very similar to the type of unbounded set of networks currently utilized by the GIG and networks. Thus, this type of higher VMP message protection could keep the GIG adaptive and functioning and assure mission objectives in the face of internal and external threats.

SONET and the GIG

The VMP approach, of course, is not the only way to assess survivability of the GIG. Expanding upon past research on Synchronous Optical Networks (SONET), Cankaya and Nair created a tool to "evaluate reliability, availability, and transient and steady-state restorability of such

[144] Sullivan, K., et al. "Information Survivability Control Systems." University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.
[145] Sullivan, K., et al.

networks."[146] This analysis is pertinent to the team's discussion of GIG survivability, and analogies between the SONET and GIG network systems can help clarify the best way to measure the overall health of the GIG. The researchers also adapted their own work on a Parametric State Reward Markov Model (SRMM/p) to characterize a metric involving reliability, availability, and restorability to determine network survivability. This does not mimic the Kazman three attributes of availability, integrity, and confidentiality, but the parallels by far outweigh the semantic differences. [147]

According to Cankaya and Nair, one of the greatest benefits of the SRMM/p analysis tool is its great flexibility. The ability to work at different conceptual levels could be key to successful GIG maintenance as the layered approach of the GIG warrants a multi-dimensional, flexible network atmosphere. The SRMM/p consists of three states: functioning, restoration, and failure.[148] The functioning state (both fully and partially functioning) tracks whether the system provides a "satisfactory amount of service to users."[149] The restoration state determines the success of recovery. If restoration completes effectively, the network goes to a functioning state; if not it enters the failure state.[150] In addition, the SRMM/p analysis tool also includes parameters to track consecutive link failures and times that the functioning performance falls below the performance threshold.[151] Using this ongoing data, the metrics track the following: reliability as the "probabilistic transient behavior" of the network's time in both functioning and restoration states; availability as the transient behavior of the network's performance in the long-run; and

[146] Cankaya, H.C., Nair, V.S.S., "A survivability assessment tool for restorable networks," IEEE 2000: 319-324.
[147] Kazman, R., et al. "The Architecture Tradeoff Analysis Method." Software Engineering Institute. 9 Mar. 2009 <http://www.sei.cmu.edu/architecture/start/publications/atam.cfm >.
[148] Cankaya, H.C., Nair, V.S.S., "A survivability assessment tool for restorable networks," IEEE 2000: 319-324.
[149] Cankaya, H.C., Nair, V.S.S.
[150] Cankaya, H.C., Nair, V.S.S.
[151] Cankaya, H.C., and Nair, V.S.S., "A survivability assessment tool for restorable networks," IEEE 2000: 319-324.

restorability as the average duration of the restoration state.[152] Table 7 shows the metrics utilized by the authors and how the system operates with input data.

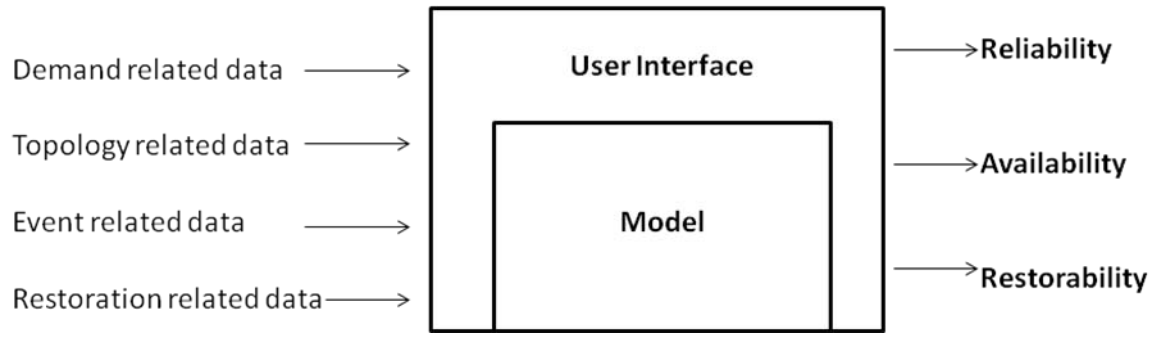

Figure 7: SONET Metric Chart Suggested By Cankaya and Nair.[153]

As seen in this chart, the model created by Cankaya and Nair serves as the focal piece of the SRMM/p analysis tool with a simple graphical user interface to make the tool user friendly. The flow-chart approach exemplifies how the data input into the user interface (on the far left) enters the model to derive parameters such as the steady-state and probabilistic transient behavior. In turn, these values aid in determining the metrics (reliability, availability, restorability) utilized.[154] Cankaya and Nair point out, however, that users who wish to start with a specific metric, such as reliability, and progress back through the SRMM/p analysis tool will have little difficulty doing so as data remains preserved for such an analysis.[155] Much of the obtained data should be entered by the user in the interface (Figure 8). Here, users enter all initial input information which eventually contributes to the parameters and threshold values. Then, users enter restoration rates and post-restoration responses. Finally, the user selects between reliability, availability, and restorability. The program then computes the desired metric alongside plotted graphs depicting

[152] Cankaya, H.C., and Nair, V.S.S.,
[153] Cankaya, H.C., and Nair, V.S.S., "Accelerated reliability analysis for self-healing SONET networks. ACM Computer Communications Review, 28.4. (October 1998): 268-77.
[154] Cankaya, H.C., and Nair, V.S.S.,
[155] Cankaya, H.C., Nair, V.S.S., "A survivability assessment tool for restorable networks," IEEE 2000: 319-324.

the information visually.[156] Accordingly, if either the failure rate increases and/or the repair rate decreases, the survivability metrics will be negatively impacted.[157] This comprehensive system can not only assess the survivability of the GIG, but also works well alongside metrics focused upon sustainability and reliability.

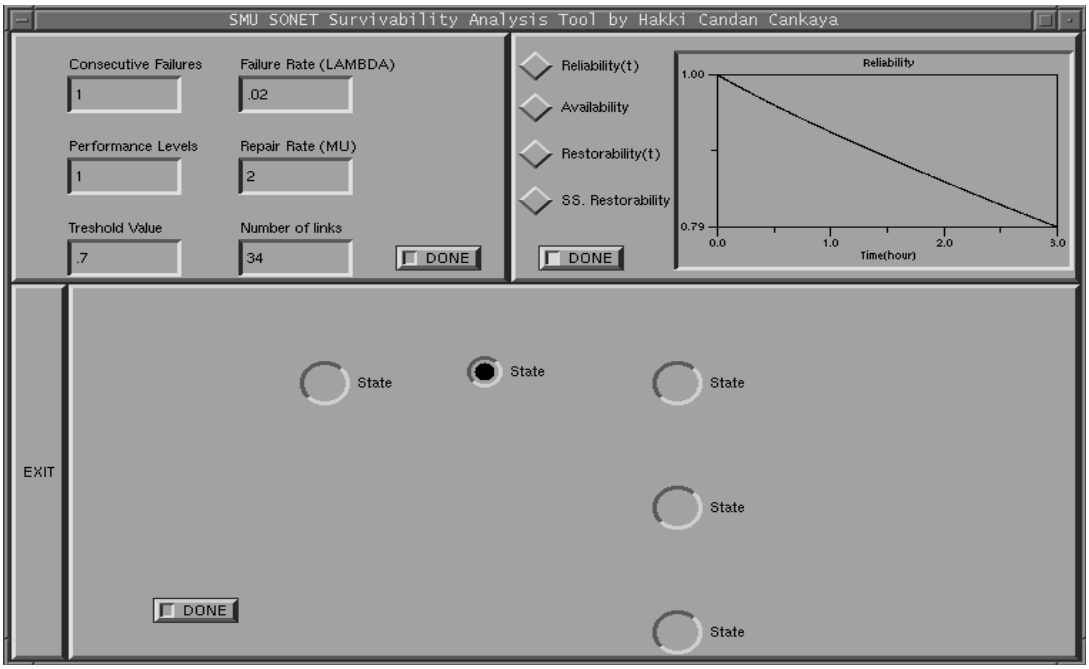

Figure 8: SONET Interface Tool[158]

Survivability in the Banking Sector

Accordingly, mission fulfillment should consider what information to maintain for a successful mission. The importance of a system within the DoD can be better explained through an analogy with the commercial banking sector. Imagine a banking computer system that contains millions of individual accounts as well as the ability to transfer funds between accounts. In this manner, it

[156] Cankaya, H.C., Nair, V.S.S.
[157] Cankaya, H.C., Nair, V.S.S.
[158] Cankaya, H.C., and Nair, V.S.S., "Accelerated reliability analysis for self-healing SONET networks. ACM Computer Communications Review, 28.4. (October 1998): 268-77.

becomes a partially unbounded network with user interaction. The "mission" on the consumers' side is to have access to personal accounts without an unmanageable amount of security. The "mission" on the banks' side is to prevent money from being stolen from both insiders and external threats.

While banks provide "a good optimization model" for systems like the GIG, the nature of protected items differs dramatically between banking and defense industries. A banking system's mission can include expected losses built into its systems, as there will be a financial loss covered by protection mechanisms such as insurance. However, the DoD's mission can be greatly compromised depending upon the *type* of information lost in a cyber attack or a system failure. Information in the GIG is heterogeneous, while money is a homogenous element. Thus, a threat model of system survivability should consider what information needs to be protected and know what is not worth the effort and burden of protection.

In addition, commercial best practices should not be automatically ruled out because there might be different goals for the defense sector versus the commercial sector. This realization of similar purpose between commercial and government entities was especially highlighted in the Clinger-Cohen Act (CCA) of 1996.[159]

The CCA is a reform act that requires the government information technology sector to work as if in the commercial industry, seeking profit while also providing efficient services to governmental consumers.[160] While the main purpose of the CCA is to prevent impulse purchases for information technology that would cost the government and accordingly the taxpayers money, its lessons also apply to the GIG. For a survivable system, there should be a focus on

[159] "Clinger-Cohen Act: The Information Technology Management Reform Act of 1996." US Department of Education. 4 May 2009 <http://www.ed.gov/policy/gen/leg/cca.html>.
[160] "Clinger-Cohen Act: The Information Technology Management Reform Act of 1996."

providing efficient services and maintaining user accessibility into the survivable system. All notions of survivability, whether part of a controlled system or not, would benefit greatly from a unitary cyber lead in charge of implementation and planning as well as maintaining a consistent set of metrics and terminology across all GIG domains.

Survivability: Commercial Best Practice

A survivable system should be adaptive in order to correct problems as they occur and anticipate problems before they evolve into a crisis. Just as computer networks demand up-to-date information, the nation's energy grids should be survivable systems able to provide power across the nation.

The survivability of the GIG is a relatively new concept, but survivability for electronic power grids has evolved over time in the commercial sector. Thus, a complete analysis of survivability in practice should look to commercial best practices of the power industry. For example, one mission of the Electrical Power Research Institute (EPRI) is to investigate "self-healing" and adaptive networks. While addressing power outages, EPRI envisions a network that can restore power to all customers within 24 minutes.

Consider an example provided by EPRI. Imagine that a tree limb falls, snapping an electrical wire and causing a power outage. In the past, a customer would alert the Operations Center that an outage had occurred. The Operations Center would contact a field technician to investigate the source of the outage. In this scenario, power would generally be restored in 40 minutes. However, with a self-healing model, an automated system would re-route power to most

customers affected by the outage within one minute. Next, the location of the outage would be pinpointed and all customers would have power restored in just 24 minutes.[161]

S. Massoud Amin, Professor of Electrical and Computer Engineering at the University of Minnesota and Director of the Center for the Development of Technological Leadership, and his colleague Bruce Wollenberg, have extensively researched self-healing or "smart grids."[162] They state that currently, "Intelligence is only applied locally by protection systems and by central control through the Supervisory Control and Data Acquisitions (SCADA) system."[163]

While the reasons to use a smart grid are numerous, there are also limitations to its implementation. For one, Amin and Wollenberg explain that the central control system is not fast enough, and the design of protection systems is too limited in their capabilities to protect only certain components. For an electrical power transmission system to have intelligence, independent processors must be part of each substation and power plant. Not only that, but they must have a "robust operating system and be able to act as independent agents that can communicate and operate with others, forming a large distributed computing platform."[164] It is important that every node within the whole system have its own sensors to monitor and assess its section with regards to its capability. These assessments should be sent to the adjacent nodes.[165]

Amin and Wollenberg offer an example to illustrate the communication between agents within an intelligent electrical power transmission system: "A processor associated with a circuit breaker would have the ability to communicate with sensors built into the breaker and communicate those sensor values using high bandwidth fiber communications connected to other

[161] Von Dollen, Don. "Enabling Energy Efficiency-IntelliGrid." Electric Power Research Institute. 19 May 2009 <http://gaia.econ.utah.edu/planning/seminar/NARUC_Intelligrid.pdf>.
[162] Massoud, Amin S., et al. "Toward a Smart Grid." IEEE Power and Energy Magazine Sept. & Oct. 2005: 34-38.
[163] Massoud, Amin S., et al.
[164] Massoud, Amin S., et al. "Toward a Smart Grid." IEEE Power and Energy Magazine Sept. & Oct. 2005: 34-38
[165] Massoud, Amin S., et al.

such processor agents."[166] The most important factor is real-time monitoring and reaction. Monitoring things such as voltage, current, and the condition of components would enable the system to regularly tune itself.[167] This approach seems akin to the VMP method already discussed.

A survivable electrical power transmission system should also anticipate problems so that the mission can be fulfilled. Computers could be made to identify warnings that occur before the onset of a disturbance, and alert human operators who could then address the situation using control features within the grid, before any ramifications have even been sent into motion.[168]

A third equally important component, isolation, is addressed by Amin and another colleague, Phillip F. Schewe. In the event of failure, the network would fragment itself into smaller sections. Each section would essentially work and repair itself. Once brought up to speed, it would reconnect to the whole network. Even though small outages would occur with sections, a widespread major blackout would be avoided.[169]

The steps that Amin and Schewe identify to begin the process of integrating an intelligent electrical power transmission system can also be applied to the GIG survivability analysis. First, a communication system must emerge that connects components of the grid (or network) and allow open communication and self-assessment. An automated system such as the one proposed by Amin and Schewe or the one implemented through VMP theory and technology would allow each piece of equipment to be monitored. Furthermore, "the millions of electro-mechanical

[166] Massoud, Amin S., et al.
[167] Massoud, Amin S., et al. "Preventing Blackouts." Scientific American May 2007: 60-67.
[168] Massoud, Amin S., et al.
[169] Massoud, Amin S., et al. "Preventing Blackouts." Scientific American May 2007: 60-67.

switches currently in use should be replaced with solid-state, power-electronic circuits, which themselves must be bolstered to handle the highest voltages: 345 kilo-volts and beyond."[170]

However, a survivable system should not only contain automated self-check and self-healing software and hardware. It should also be monitored to track external issues such as cyber threats or internal issues stemming from validated users.

Cyber Threats and Cultural Considerations

Cyber threats to the GIG vary significantly depending on an adversary's intent, technological abilities, and level of knowledge. Widespread disruption of electric service can quickly undermine the government, military readiness, economy, and endanger the health and safety of millions of citizens. In the cyber realm, denial-of-service attacks, confidential data loss, data manipulation, and system integration loss are all threats to a network.[171] Currently, government and industry policy is focused on preventing external attacks.[172] However, there is an equal or potentially more damaging threat posed by those who have inside access to information systems and networks. For example, a systems manager who does not comply with the installation patch policy could inadvertently pose as much of a threat as an external actor. Therefore, to ensure the current and future health of the GIG, it is imperative to identify vulnerabilities in the system. In today's multifaceted environment, the challenge to the battlefield is how to manage vulnerabilities and risks in order to ensure mission success. In addition, determining attacker identity (attribution) is a necessary measure as it could aid the DoD in finding methods to battle cyber threats and minimize vulnerable areas within the system. Attribution is one of the toughest

[170] Massoud, Amin S.
[171] Gansler, Jacques S., and Binnendijk, Hans. "Information Assurance: Trends in Vulnerabilities, Threats, and Technologies." National Defense University. 1 Apr. 2009 < http://www.ndu.edu/CTNSP/IAverMay03.pdf>.
[172] Gansler, Jacques S., and Binnendijk, Hans. "Information Assurance: Trends in Vulnerabilities, Threats, and Technologies." National Defense University. 1 Apr. 2009 < http://www.ndu.edu/CTNSP/IAverMay03.pdf>.

challenges in battling cyber threats, but it is crucial if the government desires to protect data in the GIG from future attacks.[173]

To assess survivability, both external cyber threats and internal issues stemming from the current defense culture should be considered. According to the DoD Architectural Vision, the GIG will drastically improve capabilities for information-sharing and increasingly allow joint forces to incorporate traditional methods with a more sophisticated approach that encompasses intelligence, surveillance, and reconnaissance.[174] Figure 9 depicts the GIG as an enabling foundation for Network-Centric Operations and Warfare (NCOW) and ultimately full spectrum dominance through increased information superiority and decision superiority.

[173] Gansler, Jacques S.
[174] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.

Figure 9: Network-Centric Warfare[175]

NCW involves "networking" in physical, information, and cognitive domains. While NCW is an operational concept, the GIG provides increased situational awareness of the network.[176] This system of systems provides functions in a global context for "processing, storage, and transport of information; human-GIG interaction; network management; information dissemination management; and information assurance."[177] The GIG significantly improves capabilities for information sharing, thus allowing joint forces to incorporate traditional methods with a more sophisticated approach that encompasses intelligence, surveillance, and reconnaissance.[178] The increased information sharing through the networking of forces underlines the importance of a

[175] U.S. Joint Forces Command. "Capstone Requirements Document: Global Information Grid (GIG)." 12 May 2009. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408877&Location=U2&doc=GetTRDoc.pdf.>.
[176] U.S. Joint Forces Command.
[177] U.S. Joint Forces Command.
[178] U.S. Joint Forces Command.

NCW environment that relies upon improvements in information operations. In addition, providing a great deal of data and capabilities to the user requires an increase in user awareness and adherence to security protocols. The U.S. government has taken practical measures to towards achieving this cultural adaptation.

The DoD recognizes GIG-related threats that could potentially compromise its networks, and has accordingly strived to provide a safer and more protected environment through updated security policies.[179] An IA tool used throughout DoD installations worldwide is the Host-Based Security System (HBSS). This tool attaches an administering device to each host—including servers, desktops, and laptops—that can be managed by local administrators who in turn can block unwanted traffic through an intrusion detection system and a host-level firewall.[180] The HBSS "features a robust white-list capability that allows use or execution of only authorized software and hardware, including peer-to-peer software, applications, USB devices and thumb drives.[181] Other system characteristics include automated support for information operation baselines, buffer overflow protection, virus system detection, and identification of unauthorized computer systems on the network.[182] While the GIG already uses heightened security measures, it could also incorporate the HBSS capability that limits access to only those with proper authorization in order to insure further data security.

HBSS was first developed in 2003 when the DoD formed the Enterprise-wide IA and Computer Network Defense (CND) Solutions Steering Group (ESSG). Its purpose is to fulfill operational requirements by incorporating and coordinating computer network defense strategies. The ESSG

[179] Gawlas, Mike. "End-Point Security Spreads Throughout Military." SIGNAL Magazine: 15 April 2009.
[180] Gorodetski, Vladimir, et al. Agent-Based Model of Computer Network Security System: A Case Study. Springer: Berlin/Heidelberg, 2001.
[181] Gawlas, Mike. "End-Point Security Spreads Throughout Military." SIGNAL Magazine: 15 April 2009.
[182] Gawlas, Mike.

is jointly led by USSTRATCOM and Joint Task Force-Global Networks Operations (JTF-GNO).[183]

The ESSG made comprehensive host-based security a priority and identified measures to uphold a specific level of protection for the department. In order to create a collaborative environment, the DoD partnered in 2006 with members of the private sector. Together, they created an automated host-based solution for system security that was designed to give network administrators and security personnel the ability to prevent, detect, track, and report any malicious cyber actions across all DoD networks and systems. [184] The ESSG also began piloting, intensive testing, certification, accreditation, and source code reviews; the same concept could be applied to the GIG, but user compliance is necessary to ensure thorough procedures are being followed.[185]

In particular, the piloting process showed the life cycle of HBSS and confirmed that successful installation and deployment most often occurs in organizations with a strong network defense workflow processes, a comprehensive knowledge of the network's infrastructure, and strong, lasting leadership.[186] Leaders, users, and operators alike concur that one malicious action against the network can impede the fulfillment of the overall mission.[187] For example, one corrupted information packet put into the network by a "stupid user trick" action can cause collateral damage to other systems. Defense Information Systems Agency (DISA) officials assert that education is key as educating network users on HBSS end-point security capabilities and other

---

[183] Rubel, Paul, et al. "Generating Policies for Defense in Depth." Paper presented at the 21st Annual Computer Security Applications Conference. 18 May 2009 <http://www.bbn.com/resources/pdf/GroupPapers_Generating-Policies-for-Defense-in-Depth.pdf>.
[184] Gawlas, Mike. "End-Point Security Spreads Throughout Military." SIGNAL Magazine: 15 April 2009.
[185] Gorodetski, Vladimir, et al. Agent-Based Model of Computer Network Security System: A Case Study. Springer: Berlin/Heidelberg, 2001.
[186] Carlberg, Ken, et al. Preferential Emergency Communications: From Telecommunications to the Internet. Kluwer Academic Publishers: Norwell, Massachusetts, 2003.
[187] Carlberg, Ken, et al.

network vulnerabilities can alleviate some of the dangers users cause by incomplete security efforts.[188]

DISA worked with DoD agencies to establish universal standards for the Nonsecure Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET).[189] Both these systems have been installed with HBSS.[190] To help combat network issues, in-person training classes and virtual training courses for system administrators were developed and put into effect. The education and training aids in setting common norms for the agency. It is important these norms include both installation techniques as well as security protocol for users to obey.

The HBSS is only one device the DoD uses to ensure IA and network defense. As stated by DISA officials, "The HBSS is just a single tool in the Defense Department's information assurance and computer network defense portfolio and is not a network security silver bullet."[191] Without skilled and diligent administrators and users, the HBSS cannot adequately fight threats to a network; this can also be correlated to the GIG. Developing simple technological capabilities is the beginning step toward achieving a complex defense strategy and will require a cultural change in user awareness. Widespread adherence to security protocols should result after completion of designated training programs and clear guidelines have been set. Users are trusted to utilize the network as they were taught in training.[192] This illustrates that the future of the GIG will rely just as heavily on cultural adaptation as it will on technological advances.

---

[188] Gawlas, Mike. "End-Point Security Spreads Throughout Military." SIGNAL Magazine: 15 April 2009.
[189] Gawlas, Mike.
[190] Gawlas, Mike.
[191] Gawlas, Mike.
[192] Carlberg, Ken, et al. Preferential Emergency Communications: From Telecommunications to the Internet. Kluwer Academic Publishers: Norwell, Massachusetts, 2003.

Another cultural consideration is the issue of user priority. Even if the network is compromised, the ultimate mission of getting necessary information to the warfighter must be fulfilled. While military rank is unquestionably an important element, mission importance should be taken into consideration and weighed heavily when deciding user priority. The decision as to who gets access to a network should not be strictly based on military rank, but should instead be based on the overall job function. A lower ranked individual should be granted access over a higher ranked individual in certain circumstances depending on the importance of the needed information. When access to a network is limited due to system integration, a ranking system could weigh rank and mission importance. Placing special emphasis on mission importance would ensure that crucial missions are accomplished. For example, a warfighter on the ground may require urgent and immediate access for survival purposes and at the same time, a high ranked officer may want to check e-mail. This example shows that it is essential that more than military rank be considered when deciding user priority.

A similar preferential ranking system has been used successfully in emergency communications. Multi-Level Precedence and Preemption (MLPP) was coined by American National Standards Institute (ANSI) to create rules and regulations within a single domain infrastructure such as emergency communications. Calls are marked with one of five priority (or precedence) levels and calls with lower priority are postponed if there was a great deal of traffic on the lines.[193] This allows calls with higher importance to be completed. The lowest precedence level is considered the default level and all levels ranked higher are considered emergency levels. The International Telecommunications Union (ITU) also used methods similar to MLPP. Each caller is responsible for accurately identifying the importance of their call at the beginning of the call. Once a

[193] Carlberg, Ken, et al.

precedence level has been chosen by the calling party, it cannot be changed. However, the next call on the same phone by the same user can be made at another authorized precedence level. Below are the established precedence values for phone calls established by the Integrated Services Digital Network (ISDN):

> The ISDN MLPP Precedence Values are:
>
> 1 “0000” = “Flash Override” (highest level)
>
> 2 “0001” = “Flash”
>
> 3 “0010” = “Immediate”
>
> 4 “0011” = “Priority”
>
> 5 “0100” = “Routine” (lowest level)
>
> “0101” – “1111” are unspecified

A circuit switched network system was created to prioritize all calls when congestion makes resources unavailable. Call preferential was determined regardless of the calling party or the called party. The concept of MLPP as designed by ANSI and the ITU was initially developed so that normal telephone traffic would not cause problems for prioritized users in the event of an emergency.[194] The GIG can use this commercial best practice as an example when determining who should have priority access to the GIG. Computer networking expert and lecturer at Johns Hopkins University, Ken Carlberg, has researched how the telephone communications example could compare conceptually to the U.S. military. The lowest level, labeled “routine,” would be

[194] Carlberg, Ken, et al. Preferential Emergency Communications: From Telecommunications to the Internet. Kluwer Academic Publishers: Norwell, Massachusetts, 2003.

considered the baseline and normal call traffic would fall into this precedence level. If a commander needed to make a basic call to reach a platoon leader, he could upgrade his call level to "priority" based on his status alone. In the event of a crisis, a commander could increase its call precedence to "immediate" or all the way to "flash override" which would guarantee that the most important commands would get access over any other traffic of any priority. However, a senior military official who is making a call without much importance is advised to use the "routine" level so that other lower ranking individuals can get through if their call is more important or pressing.[195]

An additional cultural consideration lies with the military mindset of information-sharing. As envisioned by the GIG Architectural Vision, the GIG will be a key enabler to achieving information superiority.[196] This requires a fully integrated system that incorporates joint command, control, communications, and technology must be achieved. Information sharing is also a key element to the success of network-centric operations. The Joint Forces have typically focused on information security; however, they must transition to a community of information-sharing in order to achieve complete network-centric operations. The Joint Forces is currently working to establish clear guidelines for NCO outlined in a Capstone Requirements Document (CRD) for the GIG. Here, the Joint Requirements Oversight Council would oversee the GIG and implement policy guidelines.[197]

---

[195] Carlberg, Ken et al.

[196] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.

[197] Carlberg, Ken, et al. Preferential Emergency Communications: From Telecommunications to the Internet. Kluwer Academic Publishers: Norwell, Massachusetts, 2003.

A different cultural consideration is the recognition of unitary leadership of the GIG. After talking with various experts in cyber-related fields, it was determined that a number of organizations were partially responsible for the implementation of the GIG. The current allocation of resources is also split among these governmental organizations; this can be viewed as an impediment to the overall health of the GIG because there is no unified strategy for monitoring and repairing the system. Because of gaps that could arise from this fracturing of responsibility, it has become necessary for one architectural vision to be implemented by one command to maintain the overall health of the GIG. Having one recognized organization lead the architectural vision and implementation of the GIG should greatly increase overall network performance and component compatibility.

In addition, a "revolution" in military affairs would allow for greater flexibility and information-sharing.[198] According to Metz and Kievit, this would involve a major change in the nature of warfare by applying new technology with changes in military doctrine.[199] A practical step toward a revolution in military affairs could be an incentives system that would encourage information-sharing and collaboration between the branches of the government and contributors of the GIG. This linkage between different commanders would promote global and theater integration. The combination of technological capabilities and cultural changes are necessary components to ensure the lasting health of the GIG.

[198] Metz, Steven, Kievit, James. (27 June 1995). "Strategy and the Revolution in Military Affairs: From Theory to Policy." Strategic Studies Institute. 12 Mar. 2009 < http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB236.pdf>.
[199] Metz, Steven, Kievit, James.

SYNTHESIS

Reporting Structure

While the ideal GIG consists of an interconnected, end to end set of information capabilities such as intelligence databases and missile systems, the reality of the current GIG is a fractured set of domains.[200] According to the GIG Architectural Vision, the target GIG will most likely be achieved no earlier than 2020.[201] Setting up an efficient reporting system beforehand would be crucial to ensuring a consistent measure of system health. Consequently, the effectiveness of the reporting structure could be tested and changes could be made to ensure that it would be ready in time for the target GIG.

The GIG encompasses information systems and associated personnel from departments across government and even industry. Because of the GIG's broad range of member departments and agencies, it is important that the health indicator be defined and mandated from one overarching lead entity. This should be done by first creating a list of common metric definitions and thresholds to be used across departments. Doing this would ensure consistency among all health scores, limiting the possibility of misreading the health level of a particular section of the GIG.

Although the ability to decide the identity of the Cyber Lead lies outside the scope of this report, the proposal of one central leader is crucial to the notional framework described in the following section. The concept of a Cyber Lead will be used freely to refer to the entity that will be chosen by the "proper" leadership. Optimally, this Cyber Lead would have the authority to mandate

[200] DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.
[201] DoD CIO.

consistent and universal methods of health measurement, to enforce accurate reporting, and to direct maintenance and repair.

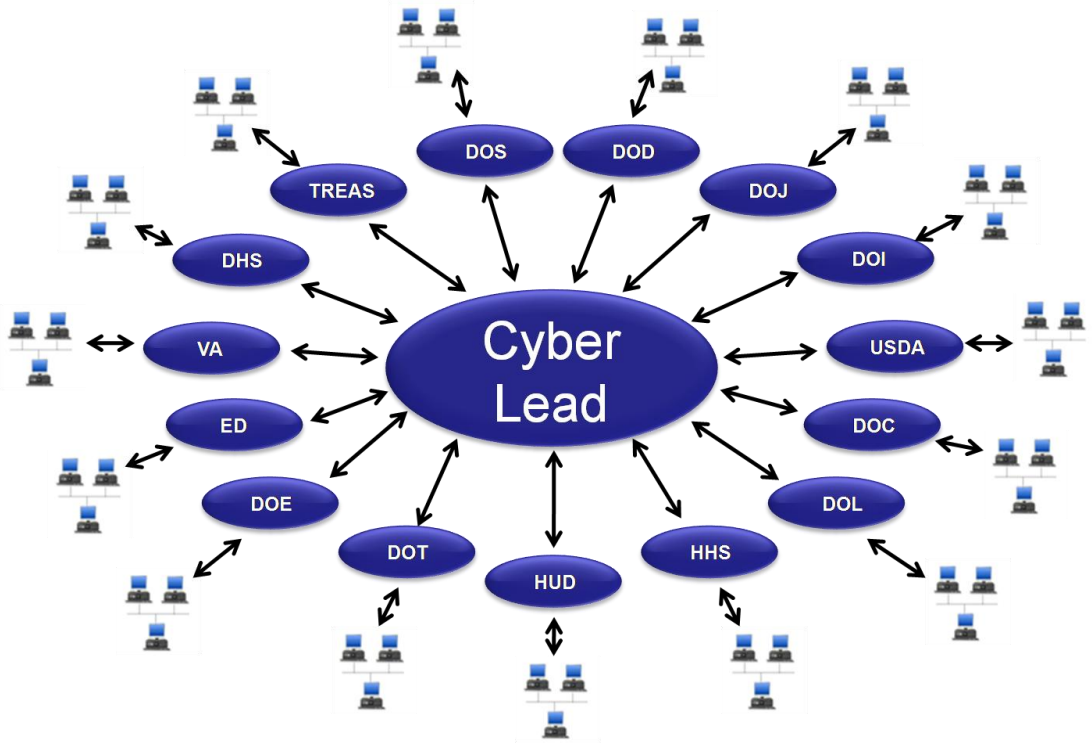

Figure 10: Notional Reporting Structure

The proposed reporting structure, shown in Figure 10, connects all levels of the GIG hierarchy. At the most basic level, each computer or device assesses itself using previously mentioned metrics such as self health checks and VMP systems. This information would then be forwarded level by level to the Cyber Lead. This hierarchical process is comparable to that of a warfighter's laptop. The laptop uses metrics to self-evaluate and sends the information to the next level: the system administrator of the warfighter's brigade or battalion. At this level, data is compiled and analyzed to extract metadata, which is then sent on to the branch level. As the data is sent up the hierarchy, it is necessary for the focus of information to move from specific devices to the

conglomeration of a set of devices. Further knowledge of the exact GIG architecture is needed to discern whether these sets are made up of a homogeneous or heterogeneous grouping of devices.

Once the measurement information is received at the branch level, the branch would calculate its own health score and send this up to the department level, which combines its score with those from other branches to formulate the department's total health score. The various cabinet positions in the government, as shown in Figure 10, such as the Department of Defense (DoD), the Department of the Interior (DoI), and the Department of Homeland Security (DHS) are akin to the prior example's department level. The Cyber Lead must know the health of each department's section, as the interconnectedness of the GIG means that an issue on one part of the network will affect the health of other sections.

Once the Cyber Lead receives the health scores from each cabinet, the information would be used to derive a health score for the overall GIG. This score would give a daily snapshot of the health and allow the Cyber Lead to scrutinize the score to identify where problem sectors lie and what management would need to do to minimize negative ramifications such as data manipulation or connectivity loss.

Notional Health Indicator

The metrics outlined in the previous sections on sustainability, reliability, and survivability would next be combined into scores for each of these sections. Methods of combining metrics will vary depending on weighting systems and the effectiveness of metrics after testing. Although research has been done on identifying and defining metrics, systems of combining

them and extracting useful information from them have not been explored extensively.[202] As a report from the National Institute of Standards and Technology states:

> The concepts of fundamental units, scales, and uncertainty prevalent in scientific metrics have not traditionally been applied to IT or have been applied less rigorously. It is also important to recognize that compared with more mature scientific fields, IT metrology is still emerging. Many physical properties began as a qualitative comparison before becoming a formally defined quantity, which holds promise for IT metrics in general.[203]

Some possible strategies for combining metrics into a comprehensive score for each section include mathematical and probabilistic models that utilize concepts such as fuzzy set theory and Artificial Intelligence (AI). Fuzzy set theory, which is a subsection of fuzzy mathematics, would allow for a fluid weighting system and partial set memberships. Unlike in classical set theory where an element is either contained or not contained in a set, fuzzy set theory allows an element to have a fractional membership by using a membership function that produces values in the real number interval from 0 to 1 ([0 , 1]). In this way, an element is fully a member of the set if it produces a 1 in the membership function, and not a member if it produces a 0. Any value in between 0 and 1 indicates partial membership.[204] Fuzzy set theory could be utilized to weight the individual metric scores in order to create an overall score for each criterion. This could be achieved by determining a membership function of metric effectiveness to indicate the level of membership in a set which would be utilized to create the score.

---

[202] Jansen, Wayne. "NISTIR 7564: Directions in Security Metrics Research." National Institute of Standards and Technology, 31 Mar. 2009 < http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>.
[203] Jansen, Wayne.
[204] Mordeson, John N., and Premchand S. Nair. Fuzzy Mathematics: An Introduction for Engineers and Scientists. Physica-Verlag: New York, 2001.

Another strategy is to explore the use of AI, which has been the focus of much research in the technology industry recently. As discussed in the sustainability section, a semi-quantitative approach to health measurement is necessary. This combination of qualitative and quantitative analysis lends itself to the idea of AI which "involves the design and implementation of systems that exhibit capabilities of the human mind, such as reasoning, knowledge, perception, planning, learning, and communication."[205] By using AI, the qualitative analysis could become automated, which would allow for a quicker and more objective measurement.

When creating a system to combine metrics, it is important to weigh the metrics based on their accuracy and importance as some metrics reflect more critical measures of health than others. Also, the purpose of the device should be taken into consideration. While a GPS device is without a doubt important to the warfighter in the field, a server that handles missile systems affects more people and should therefore be watched more carefully and weighed more heavily. It is essential to keep in mind that regardless of strategy, the method of combining metrics to create a score should be validated through testing on the GIG system.

[205] Jansen, Wayne. "NISTIR 7564: Directions in Security Metrics Research." National Institute of Standards and Technology, 31 Mar. 2009 < http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>.

Criterion	Weight	Score	Total
Sustainability	0.3		
Reliability	0.3		
Survivability	0.4		

Figure 11: Notional Health Indicator

Figure 11 shows the basics of the notional Health Indicator created by the team. The scores for sustainability, reliability, and survivability are determined and then weighed using the values shown in the table. Sustainability is worth 3/10 of the total score, and refers to the percent of hardware and software that is operating effectively. Reliability is also worth 3/10, and reflects both the ability to access information in a timely manner and the level of assurance that the information accessed is accurate. Survivability is worth 4/10 of the final score, and indicates the probability that the system continues to operate during a network failure or attack.

Although all three sections are important to GIG health measurement, survivability is weighted more heavily than sustainability and reliability. This is because survivability concerns the GIG's

capability to fulfill its mission and to a certain extent has sustainability and reliability inextricably intertwined within it. As General Chilton said at the 2009 Cyberspace Symposium, "the most difficult challenge is continuing to operate our networks when we come under attack."[206] Because the GIG provides information and capabilities necessary for national defense, it can be considered a weapon in itself. The consequences of an information breach could cost the U.S. both millions of lives and dollars. Therefore, even in the event of an attack or failure, the GIG must continue to operate.

The sub-score for sustainability, reliability, and survivability provide a reading that tells the administrator how the system rates in each area. The scores change from day to day, and provide a more focused look at where problems are in the GIG. The administrator would use this information to delve further into the health score, separating the score into its relative sections, and into the hierarchy to pinpoint problem locations. This information could be used to make operational and tactical decisions, from isolating problem sectors to determining where to focus for maintenance and repairs.

[206] Chilton, Kevin P. (2009, April). Opening Remarks. *USSTRATCOM Perspective*. Symposium conducted at the meeting of the 2009 Cyber Symposium, Omaha, Nebraska.

Criterion	Weight	Score	Total
Sustainability	0.3	96	28.8
Reliability	0.3	95	28.5
Survivability	0.4	96	38.4
			95.7

Figure 12: Notional Health Indicator Example

The notional example created by this team, as shown in Figure 12, illustrates how the Health Indicator would display scores for one day. In this instance, sustainability, with a score of 96 indicates that most of the hardware in the GIG is operating effectively, software is up to date, and both can be expected to sustain for the current day. Reliability's score of 95 means that most of the data is and will remain accurate and accessible for the current day. Sustainability has a score of 96, which signifies there is a high probability that the GIG will continue to operate in the event of attack or network failure. The score shown at the bottom right is the total health score that is the result of combining the three weighted sub-scores.

Notional Health Index

The notional health index provides a simple picture of GIG health to the Cyber Lead each day. It takes the notional health indicator total score and places it numerically in the notional health index (Figure 13) to display the overall GIG health level. Here, the Health Index mirrors the triage system used by emergency room technicians to assess a patient's condition quickly and determine the amount of resources and manpower needed to address the situation.

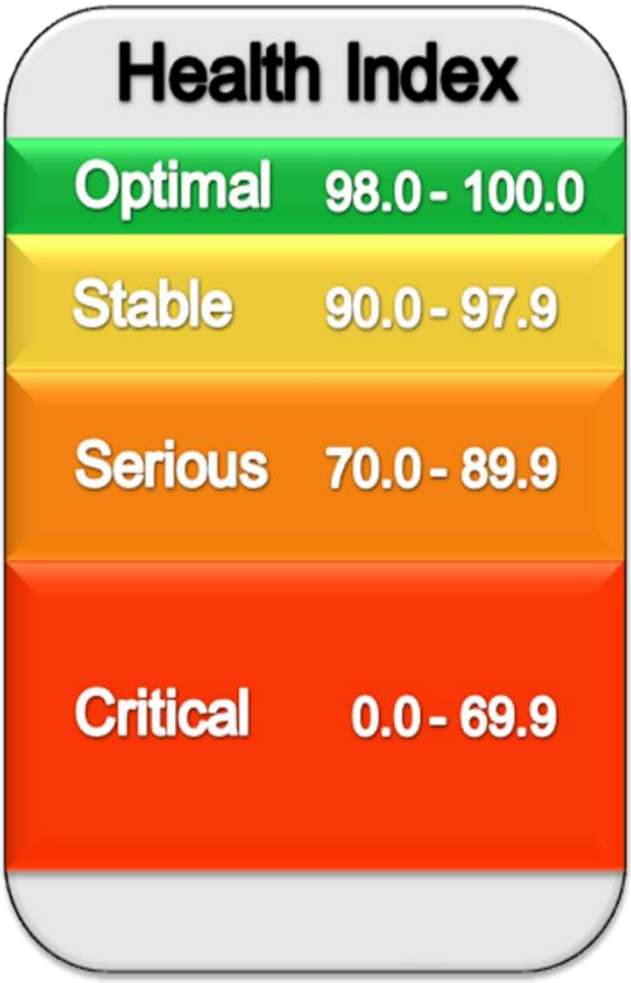

Figure 13: Notional Health Index

When examining the Health Index, it is important to keep in mind that the numbers located on the right side refer to the score determined from the notional Health Indicator, not an overall

percentage of the GIG that is operational. The optimal level, indicated by the color green, signifies the system is healthy overall and just basic, everyday maintenance is required. This level is shown as the smallest of the four, indicating that a score in the optimal level is the rarest. The stable level, indicated by the color yellow, signifies that a few incidents are occurring that require attention to prevent further system degradation. The serious level, indicated by the color orange, signifies a situation is occurring that requires immediate attention to prevent widespread impact on GIG operations. The critical level, indicated by the color red, signifies a major event is occurring that will cause a critical widespread reduction in capability.

This Health Index score would tell the Cyber Lead the daily health level of the GIG. Testing of the framework on the GIG hardware is vital to establishing a baseline. From this it can be determined where an everyday, normal reading of health will lie along the spectrum. The Cyber Lead can then examine the health score of the day and dissect it to show the three sub scores if needed. If the score is unsatisfactory, it is possible to follow the line of reporting back to the appropriate level to identify a problem. This makes it easier for maintenance and repair decisions to be made.

CONCLUSION

Extensive, multi-faceted analysis of maintaining the health of a complicated network called the GIG has led to a series of recommendations. Through speaking with experts in academic, government, and commercial sectors, and through reading publications from relevant experts, it is uncontested that the health of a network must include analyses of the network's sustainability, reliability, and survivability. In addition, the team examined the commercial sector to determine what commercial best practices existed to maintain the health of a large network such as the GIG. Overall, these three essential components demand a framework of relevant metrics, as suggested in this report. However, the health analysis cannot stop there. Previous methods to track the health of the GIG remain complicated, providing multiple measures and assessments that do not combine to an overall health score which can be readily examined. Thus, this report not only suggests reliable metrics to measure sustainability, reliability, and survivability, but also proposes an overall framework for these metrics through a notional model. The notional model considers these three components, with weighted averages, and combines them into an overall GIG health score that is then examined in relation to the overall Health Index. Again, the analysis does not stop there. A helpful framework with relevant metrics measures essential components is useless without the personnel and network capability required to maintain and determine such a score. The defense culture must be examined to (1) enforce collaboration among organizations that contribute information to the GIG and (2) ensure user accountability. The GIG is not just an informational web site like Google.com. Instead, it is a weapon that must be protected. Acknowledged unitary control of the GIG can help protect the network and also aid

in implementing health indicators and overall health scores to ensure that the GIG not only remains healthy, but also can adapt over time to meet the new, emerging needs of the US.

BIBLIOGRAPHY

Acohido, Byron and Swartz, Jon. "Botnets can be used to blackmail targeted sites." USA Today. 17 Mar. 2008. <http://74.125.95.132/search?q=cache:fck5veGX_HEJ:www.usatoday.com/tech/news/computersecurity/2008-03-16-botside_N.htm+%22Botnets+can+be+used+to+blackmail+targeted+sites%22+%26+Swartz&hl=en&gl=us&strip=1>.

Air Force. "Military Handbook for Reliability Prediction of Electronic Equipment." Quanterion Solutions Incorporated. 1 May 2009 <http://www.quanterion.com/Publications/MIL-HDBK-217/MIL-HDBK-217F%20w%20N1%20and%20N2.pdf>

Anderson, T. and Randell, Brian. "System Reliability and Structuring." Computing Systems Reliability. CUP Archive (1979): 1-18.

"Availability and description of the File Checksum Integrity Verifier utility." Microsoft Help and Support. 14 May 2009 <http://support.microsoft.com/kb/841290>.

Bhaiji, Yusuf. "Network Security Technologies and Solutions." Network World. 20 Apr. 2009 <http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html>.

Bittau, Andrea. "WiFi Exposed." Crossroads. 25 Jun. 2009 <http://www.acm.org/crossroads/xrds11-1/wifi.html>.

Braden, R., Clark, D., and Shenker, S. Integrated Services in the Internet Architecture: an Overview. Internet Engineering Task Force Documents. 30 Apr. 2009 <http://tools.ietf.org/html/rfc1633>.

Buda, Gary, et al. "Security Standards for the Global Information Grid." IEEE. 21 Jan. 2009 <http://http://ieeexplore.ieee.org.leo.lib.unomaha.edu/stamp/stamp.jsp?tp=&arnumber=985877&isnumber=21247>.

Burbeck, K., et al. "Time as a Metric for Defence in Survivable Networks."Computer Science at the University of Virginia. 15 Mar. 2009 < http://www.cs.virginia.edu/~zaher/rtss-wip/19.pdf >.

Cankaya, H.C., and Nair, V.S.S., "Accelerated reliability analysis for self-healing SONET networks. ACM Computer Communications Review, 28.4. (October 1998): 268-77.

Cankaya, H.C., and Nair, V.S.S., "A survivability assessment tool for restorable networks." IEEE 2000: 319-324.

Carlberg, Ken et al. Preferential Emergency Communications: From Telecommunications to the Internet. Kluwer Academic Publishers: Norwell, Massachusetts, 2003.

Chaplain, Cristina, et al. "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation." U.S. Government Accountability Office. 13 May 2009 <http://www.gao.gov/new.items/d04858.pdf>.

Chilton, Kevin P. (2009, April). Opening Remarks. *USSTRATCOM Perspective*. Symposium conducted at the meeting of the 2009 Cyber Symposium, Omaha, Nebraska.

Cisco. "Understand and Strengthen Your Organization's Security Architecture." Cisco Security Architecture Assessment Service. 16 May 2009 <http://www.cisco.com/en/US/services/ps2961/ps2952/cisco_saa_ds.pdf>.

"Clinger-Cohen Act: The Information Technology Management Reform Act of 1996." US Department of Education. 4 May 2009 <http://www.ed.gov/policy/gen/leg/cca.html>.

DoD CIO. "Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise Version 1.0." U.S. Department of Defense. 13 May 2009 <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>.

"E-Class Solutions: Affordable Enterprise Performance." SonicWALL, Inc. 16 May 2009 <http://www.sonicwall.com/us/products/7523.html>.

Ellison, R.J., et al. “Survivable Network Systems: An Emerging Discipline.” CMU/SEI-97-TR-013 Technical Report. 1 May 2009 <www.cert.org/research/97tr013.pdf>.

Gallegos, Arthur, et al. “Space Acquisitions: GAO-06-537 Space Acquisitions: DoD needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications Systems.” U.S. Government Accountability Office. 16 May 2009 <http://www.gao.gov/new.items/d06537.pdf>.

Gansler, Jacques S., and Binnendijk, Hans. “Information Assurance: Trends in Vulnerabilities, Threats, and Technologies.” National Defense University. 1 Apr. 2009 < http://www.ndu.edu/CTNSP/IAverMay03.pdf>.

Gawlas, Mike. “End-Point Security Spreads Throughout Military.” SIGNAL Magazine: 15 April 2009.

Gerstle, Don. "Burn-In Issues." Electronic Design. 17 Apr. 2009 <http://europe.elecdesign.com/Articles/ArticleID/10777/ 10777.html>.

“Global Information Grid Digital image.” Wright-Patterson Air Force Base. 17 May 2009 <http://www.wpafb.af.mil/shared/media/photodb/photos/060629-F-7777J-025.jpg>.

Gorodetski, Vladimir, et al. Agent-Based Model of Computer Network Security System: A Case Study. Springer: Berlin/Heidelberg, 2001.

Hubenko, Victor P., et al. "Improving the Global Information Grid's Performance through Satellite Communications Layer Enhancements." IEEE Communications Magazine Nov. 2006.

"Human Error, Not Software, the Main Cause of Network Failure." ComputerWeekly.com. 17 May 2009 <http://www.computerweekly.com/Articles/2004/02/10/200073/human-error-not-software-the-main-cause-of-network.htm>.

"Information Assurance." National Information Assurance Glossary. Committee on National Security Systems. 5 June 2009 <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.

Information Sciences Institute, University of Southern California. “Internet Protocol: DARPA Internet Program Protocol Specification.” RFC: 791. 20 Apr. 2009 <http://tools.ietf.org/html/rfc791>.

Jansen, Wayne. “NISTIR 7564: Directions in Security Metrics Research.” National Institute of Standards and Technology, 31 Mar. 2009 < http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>.

Kay, Russell. "MTBF." Computer World 31 Oct. 2005: 30.

Kazman, R., et al. “The Architecture Tradeoff Analysis Method.” Software Engineering Institute. 9 Mar. 2009 <http://www.sei.cmu.edu/architecture/start/publications/atam.cfm >.

Klein, Jay. "The ABCs of Traffic Management." CommunicationsNews. 30 Apr. 2009 <http://www.comnews.com /features/2008_july/0708_beyond_testing.aspx>.

Luddy, John. “The Challenge and Promise of Network-Centric Warfare.” Lexington Institute. 16 May 2009 <http://www.lexingtoninstitute.org/docs/521.pdf>.

Massoud, Amin S., et al. "Preventing Blackouts." Scientific American May 2007: 60-67.

Massoud, Amin S., et al. "Toward a Smart Grid." IEEE Power and Energy Magazine Sept. & Oct. 2005: 34-38.

Mell, Peter, et al. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." Global Initiatives. 12 May 2009 <http://www.first.org/cvss/cvss-guide.html>.

Melvin, Stephen R. Personal Interview. 31 Mar. 2009.

Menard, Philimar. "Reliability vs. Availability: Clearing up misconceptions." Communications Technology. 12 Mar. 2009 <http://www.cable360.net/ct/operations/bestpractices/Reliability-vs-Availability_33189.html>.

"mental hygiene." Encyclopædia Britannica. 1 May. 2009 <http://www.britannica.com/EBchecked/topic/375371/mental-hygiene>.

Metz, Steven, Kievit, James. (27 June 1995). “Strategy and the Revolution in Military Affairs: From Theory to Policy.” Strategic Studies Institute. 12 Mar. 2009 <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB236.pdf>.

Mordeson, John N., and Premchand S. Nair. Fuzzy Mathematics: An Introduction for Engineers and Scientists. Physica-Verlag: New York, 2001.

NIST/SEMATECH. "'Bathtub' Curve." Engineering Statistics Handbook. 24 July 2009 <http://itl.nist.gov/div898/handbook/apr/section1/ apr124.htm>.

"Packet loss or latency at intermediate hops." Nessoft Knowledge Base. Nessoft. 14 May 2009 <http://www.nessoft.com/kb/24>.

"physical fitness." Encyclopædia Britannica Online. 1 May 2009 <http://www.britannica.com/EBchecked/topic/458677/physical-fitness>.

Prasad, R. S., et al. “Bandwidth Estimation: Metrics, Measurement Techniques, and Tools.” College of Computing Georgia Tech. 26 June 2009 <http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/Papers/NetDov0248.pdf>.

Rist, Oliver. "Stupid User Tricks: 11 IT Horror Stories." InfoWorld 13 Apr. 2006. 18 May 2009 <http://www.infoworld.com/d/adventures-in-it/stupid-user-tricks-eleven-it-horror-stories-822>.

Rubel, Paul, et al. "Generating Policies for Defense in Depth." Paper presented at the 21st Annual Computer Security Applications Conference. 18 May 2009 <http://www.bbn.com/resources/pdf/GroupPapers_Generating-Policies-for-Defense-in-Depth.pdf>.

Satterthwaite,Charles P. “Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid.” Defense Technical Information Center. 13 May 2009 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468199&Location= U2&doc=GetTRDoc.pdf>

Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., 1996.

"Secure Socket Layer (SSL): How It Works." VeriSign. 30 Apr. 2009 <http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/index.html>.

"Secure Socket Layer Virtual Private Network." Bitpipe.com. 25 May 2009 <http://www.bitpipe.com/tlist/SSL-VPN.html>.

Sullivan, K., et al. “Information Survivability Control Systems.” University of Virginia Department of Computer Science. 5 Mar. 2009 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7943>.

Talbot, David. "The Internet Is Broken." Technology Review. 24 June 2009 <http://www.technologyreview.com /article/16356/>.

“The Wisdom of Simple Security.” CommunicationsNews. 31 Mar 09. <http://www.comnews.com/features /2008_September/0908_coverstory.aspx>.

US-CERT. “Vulnerability Summary for the Week of December 10, 2007.” Cyber Security Bulletin SB07-351. 13 May 2009 <http://www.us-cert.gov/cas/bulletins/SB07-351.html>.

US Joint Forces Command. Capstone Requirements Document: Global Information Grid (GIG). 12 May 2009. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408877&Location=U2&doc=GetTRDoc.pdf>.

“Using Ipswitch WhatsUp Gold v12.4.” University of Nebraska at Omaha. 26 June 2009 <https://whatsup.unomaha.edu/NmConsole/Help/1033/index.htm?Browser_Check.htm?toc.htm>.

Varshney, Upkar, et al. "Measuring the Reliability and Survivability of Infrastructure-oriented Wireless Networks." IEEE (2001) 611-18.

Varshney, Upkar,et al. "Patient Monitoring Using Ad Hoc Wireless Networks: Reliability and Power Management." IEEE Communications Magazine 2006: 2-8.

Vernon P.E. “Some characteristics of the good judge of personality.” Journal of Social Psychology. 4(1933): 42–57.

Von Dollen, Don. "Enabling Energy Efficiency-IntelliGrid." Electric Power Research Institute. 19 May 2009 <http://gaia.econ.utah.edu/planning/seminar/NARUC_Intelligrid.pdf>.

Ware, Willis. “Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security.” National Institute of Standards and Technology. 20 Apr. 2009 <http://csrc.nist.gov/publications/history/ware70.pdf>.

Westmark, V. R. “A Definition for Information System Survivability.” Proceedings of the 37th Hawaii International Conference on System Sciences. 5 May 2009 <http://www2.computer.org/plugins/dl/pdf/proceedings/hicss/2004/2056/09/205690303a.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253A72.166.249.2 >.

"WhatsUpGold." University of Nebraska at Omaha. 14 May 2009 <http://whatsup.unomaha.edu>.

White, B. E. “Layered Communications Architecture for the Global Grid.” MITRE Corporation. 13 May 2009 < http://www.mitre.org/work/tech_papers/tech_papers_01/white_layered/white_layered.pdf>.

Wolfowitz, P. “Global Information Grid (GIG) Overarching Policy.” Department of Defense Directive 8100.1. 13 May 2009 <http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf>.

World Health Organization. “WHO Definition of Health.” Constitution of the World Health Organization: Preamble. 13 May 2009 < http://www.who.int/about/definition/en/print.html>.

APPENDIX A

Survivability definitions from Westmark (2004).

[1] The survivability model has three states: functioning (satisfactory amount of service to users), restoration (where recovery procedure takes place), and failure (the opposite state is functioning). The evaluation of survivability uses three metrics and their probabilistic values: reliability ("transient behavior of the model's functioning and restoration states with the integration of the states' reward values"), availability ("steady-state behavior of the same states with the same performance integration"), and restorability ("average amount of recovery and average restoration duration"). Simulated the New Jersey network with 11 nodes and 23 links. The results supported survivability of a network is affected by the restoration time and the amount of recovery after restoration. SUMMARY: Survivability is measured by reliability, availability and restorability.

[2] Authors use trellis graphs to find disjoint routing paths of network systems, which can be used to address survivability. Focus is on shortest path, which minimizes delay, minimization of bandwidth, and maximization of bandwidth. "Survivability techniques are classified as 1) prevention, 2) network design, and 3) traffic management and restoration." The proposed algorithm transforms a network to a trellis graph then finds the k-best path through the trellis. This in turn is transformed into a Minimum Cost Network Flow (MCNF) problem. SUMMARY: Survivability is measured by connectivity.

[3] Analyzes survivability of network systems, which are service dependent; therefore a system architect should focus on the design of the system by analyzing only the service required of that system. The authors of this paper use a Constrained Markov Decision Process (CMDP) to form the basis of the survivability analysis, which is composed of reliability, latency, and cost-benefit. The survivability analysis process, using techniques such as model checking, Bayesian techniques, probabilistic techniques, and cost-benefit analysis, is covered in six steps: 1) Model the network using a finite state machine, 2) Inject faults into the model annotated by a special state variable with specified assumptions, 3) Specify survivability properties classified by faults (where a service node may reach an undesired or unsafe state) and services (where an issued service is monitored for completion of that particular service, which eventually does complete), 4) Construct fault scenario graphs and use model checking. Since the graphs can get quite large a querying process was developed to select a subset of scenarios that represent the events of interest to the architect, 5) Perform the reliability and latency analysis by assigning a Boolean variable to each state (indicating if an event occurred), a conditional probability (indicating probability of reaching a state), and a cost to the edges. The reliability metric is the probability that an event will eventually finish and the latency metric is the time to complete the event, and

6) Perform cost-benefit analysis to possible improvements to links based on cost, reliability, and latency. The analysis can identify critical nodes and determine survivability of a system with respect to the properties: fault and services. A tool, Trishul, was developed to simulate the basic algorithms presented in the paper. SUMMARY: Survivability is measured by reliability, latency, and cost-benefit.

[4] A class of traffic-based survivability measures is defined, where the performance of the network is used as the analysis of survivability. Networks are evaluated with and without restoration. Mentions two types of survivability measures: 1) "deterministic survivability measures depend solely on topology of the network", 2) "probabilistic survivability measures depend on topology and reliability of each component on the network, which is further split into connectivity-based and traffic-based measures." The authors use a model that is an undirected graph of nodes and links with probabilities that the link and/or node are operative. The analysis is used to find three measures of survivability: 1) "Terminal survivability: the fraction of traffic between a specific pair of nodes that can be carried by the network", 2) "Network survivability: the fraction of traffic of the entire network that can be carried by the network," 3) "Subnet survivability: the fraction of traffic of a subnet that can be carried by the network." NOTE: 4 pages of the 8 pages were missing from the PDF file. SUMMARY: Survivability is measured by network performance.

[5] Assesses and analyzes survivability based on a survivability framework. A threshold is determined for acceptable level of network performance in the context of user expectations. Outages have three major features: 1) unservability 2) duration 3) weight, which fall into three major categories: 1) catastrophic, 2) major, and 3) minor. Two approaches to survivability analysis: 1) "Probability of network failure and rates of repair to calculate network availability or unservability." and 2) "Measures of a network after a given failure has occurred using probabilistic weighting of the resulting states of the network and resulting restored after the failure." In the context of a telecommunications network at the service layer, "survivability measures may include end-to-end grade of service, number of calls, number of connected subscribers, network operator's revenue and traffic volume." SUMMARY: Survivability measurements are to be determined by the analyst.

[6] The authors use the Monte Carlo simulation and reliability algorithms to determine the probability of a surviving connection for node pairs. Probabilities are assigned to edges of a network graph. The simulation randomly generates graphs of a network system with the nodes predefined to represent the system. The minimum reliability value of the node pairs in the system is used as the network survivability value. SUMMARY: Survivability is measured by connectivity and assigns the lowest reliability value between node pairs as the network survivability value.

[7] A survivability function is used as the measure instead of a single value for survivability. The author evaluates network survivability in terms of nodes connected after a failure (disaster) that

results in unavailable or destroyed nodes. The survivability function is described as “the probability that a fraction of the nodes are connected to the central node.” The function allows for different quantities to be calculated based on the network characteristics such as type of failure (disaster) and goodness of the network. The survivability function can calculate expected, worst-case, r-percentile, and probability of zero survivability. SUMMARY: Survivability is calculated as a function that depends on the type of network failure and the remaining links available after the failure.

[8] Survivability is measured by traffic capacity, not network connectivity. Survivability is calculated as a percentage of remaining network traffic flow to the original traffic after the communication network has been destroyed. SUMMARY: Survivability is measured by traffic capacity.

[9] Measures survivability in formulas as vectors in terms of cutsets. A cutset is “a set of edges whose removal results in a disconnected network.” The computation of survivability limits the number of cutsets and classifies two types of problems: 1) minimum cutsets and 2) weakest cutsets. SUMMARY: Survivability is formulated as vectors in terms of cutsets.

[10] The authors propose a model to assess the survivability of a network system. Different parameters affect survivability such as the frequency and impact of attacks on a network system. The measure of survivability = (performance level of the new state of the system after and attack)/(system performance at a normal level). The possible values of survivability range from 1 (completely normal) to 0 (failure). Another possible calculation is a weighted sum of the importance level of the service times the degree of compromise of the service in the survived state. The authors finally conclude that there is no “absolute survivability” and sites other measures of survivability such as relative survivability, worst-case survivability, and survivability with expected compromise. Simulations to analyze survivability used the Poisson model. SUMMARY: Survivability is calculated in terms of network performance.

[11] Survivability is analyzed using the Steiner network problem, which addresses connectivity of a network system under node and link failures. SUMMARY: Survivability is measured by connectivity.

[12] Measure for survivability is based on topological structures of network systems, specifically military communications networks (MCNs). The measure of survivability is based on connectivity where measures make the following assumptions: 1) nodes have only two status, damage or undamaged, 2) links between nodes are wireless, 3) only one node is destroyed or moved at a time SUMMARY: Survivability is measured by connectivity.

[13] Survivability is computed as the probability that communication across a network is a success. The indexes are based on a function of actions causing the network to be down. The authors use Boolean algebra, probability, and queuing theories to support the computation of

survivability. SUMMARY: Survivability is measured by success of communication (network performance).

[14] Survivability is calculated as network performance where the fraction of time in failure state affects the performance. The authors choose measure performance as a time interval, called traffic blocking level, versus using perceived service effects as a measure. The magnitude, duration, and frequency of failure are used to determine the impact to traffic performance. SUMMARY: Survivability is calculated as network performance.

[15] The authors use capacity related reliability (CRR) for the survivability index and developed a tool called SACHEL (Survivability Analysis of complex Computer networks with Heterogeneous Link-capacities) to perform the survivability analysis. Networks are graphed as nodes (services) and links (connection services). SUMMARY: Survivability is calculated as network capacity.

[16] Elaborates on the computation of the survivability metric called the Node Connectivity Factor (NCF). NCF is concerned with the remaining nodes after a connection to nodes or links fail. The authors introduce knowledge-based computations to determine the NCF values for networks with large amounts of nodes (greater than 15). "The final NCF value can be formed by combining the NCF values determined for subgraphs at lower levels." SUMMARY: Survivability is measured by connectivity.

[17] The terms connectivity and survivability are used interchangeably in this article. The author measures survivability using Node Connectivity Factor (NCF) and Link Connectivity Factor (LCF). For a survivable network, high values of NCF and LCF are ideal. NCF represents the physical stability and LCF represents the electronic stability.

Probabilistic values are assigned to nodes and links. A modified cut-saturation algorithm in conjunction with Floyd's algorithm is used in the design process for networks. Inputs to the algorithm include: network topology, traffic flow, and traffic requirements between pairs of nodes. SUMMARY: Survivability is measured by connectivity.

[18] Authors "identify real-time metrics to quantify system survivability" and propose data visualization. Analysis of survivability depends on system performance during three states of failure: 1) period after failure, period during failure, and period following recovery of failure. The calculations are too specific to the mobile network system. SUMMARY: Survivability is measured by network performance.

ABOUT THE AUTHORS

Jason Cantone graduated from the University of Nebraska College of Law with his J.D. and M.A. in Psychology and is currently a doctoral candidate in Law and Psychology. His published research focuses upon decision making in both public policy (*Missouri Law Review, Journal of Experimental Psychology-Applied*) and legal contexts (*Drake Law Review*). Jason will transition from this internship to a position at U.S. Strategic Command at Offutt AFB.

Natasha Fields is a junior at the University of Nebraska at Omaha, studying Psychology, International Studies, and Spanish. She is the recipient of several scholarships for academic achievements, most notably the Goodrich, and is an active member of the honors program at the university. Natasha plans to continue excelling in her fields of study as well as spend several semesters abroad.

Brandon Iske is a senior at the University of Nebraska at Omaha studying Computer Science with a concentration in Information Assurance. He is a technical person who loves hands-on work and troubleshooting. Brandon is originally from Grand Island, NE. He enjoys working with computers and any new technology; he also enjoys anything automotive. With a concentration in Information Assurance, security has become a big area of focus and interest. He wants to make a difference and improve the world.

Kristin Phaneuf is a senior at Creighton University majoring in International Relations. She plans to attend law school where she can specialize in international law. She is the recipient of Creighton's Magis Scholarship for exceptional leadership and service to the community as well as the Ignatian Scholarship for her academic achievements. Kristin will transition from the GISC to a position at U.S. Strategic Command's Joint Exercises and Training Branch

Karen Poyer recently graduated from Creighton University with a Bachelors of Science in Mathematics. While at Creighton she also minored in Computer Science and Vocal Music, in addition to being on the executive team of organizations such as the Inter Residence Hall Government, New Student Orientation, Creighton Student Admissions Representatives, and the Creighton Center for Service and Justice's Spring Break Service Trip Program. Karen is currently pursuing employment in the National Intelligence Community.

Daniel Reynoso is a senior at the University of Nebraska at Omaha and is currently studying Psychology with a minor in Religious Studies. He plans to earn his Masters degree in Cognitive Psychology and is interested in studying the mental processes behind reading, especially in the area of sacred texts.

Ann Sawatzki is a recent graduate of the University of Nebraska at Omaha with a Bachelors of Science in Political Science. While at the University of Nebraska, Ann was Vice President of her

social science honor society, Pi Gamma Mu, and a recipient of the Peter Kiewit Scholarship for her academic excellence.